# IWS Biometric Engine®
## Securing the Future

## "An identity is stolen every 3 seconds"

*-Digital Journal*

## "Over 80% of organizations are victims of fraud"

*-SANS Institute 2013*

## IDENTITY IN THE 21ST CENTURY

The lack of identity management currently costs businesses and individuals billions of dollars every year and has sobering consequences for national security. From our borders to our banks, there have been countless instances of identity fraud. According to a survey released by the Federal Trade Commission in September 2003, 27.3 million Americans had been victims of identity theft in the previous five years. In the final year alone, it was deemed that businesses, financial institutions and consumer victims had lost $53 billion due to identity theft. Furthermore, victims' names and other identifying information were used to open new accounts, falsely obtain official documents, obtain medical care or employment and obtain government documents such as passports.

## IMAGEWARE® SYSTEMS (IWS) SOLUTIONS FOR IDENTITY MANAGEMENT

ImageWare Systems (IWS) understands what it takes to properly identify a person. IWS has over 13 years of experience in developing proven software solutions for the creation and issuance of highly secure documents such as driver licenses, national ID cards, passports and voter registration cards. IWS has been providing law enforcement with biometric solutions that facilitate and speed the criminal suspect identification process since 1997. Building on these strengths, IWS developed the IWS Biometric Engine® to enable government agencies and private enterprise to verify the identities of people quickly, easily and efficiently.

## IWS BIOMETRIC ENGINE

The IWS Biometric Engine is a scalable, agnostic omni-biometric identity management solution that delivers non-refutable proof of identity and ensures only valid individuals gain access to controlled areas or attain secure documents. The IWS Biometric Engine is available as part of a Web-based, biometric enrollment and identity verification application. It is also available as a software developer's kit (SDK) that enables system integrators to build custom identity verification applications or incorporate biometric enrollment, search and authentication functionality into existing applications.

The IWS Biometric Engine conducts 1:1, 1:N, N:N and X:N searching options; is agnostic in biometric algorithm and hardware (omni-biometric); and retains the captured biometric image to ensure that biometric algorithms can be easily changed. Additionally, the IWS Biometric Engine can manage tens of millions of individuals using standard off-the-shelf hardware, minimizing the cost of ownership.

Most importantly, the IWS Biometric Engine provides indisputable proof of identity across large-scale populations and distributed enterprises conveniently, inexpensively and securely, and can be integrated into a variety of applications which can be deployed in a wide array of various industries.

The IWS Biometric Engine is based on field-proven IWS technology that has been used to manage millions of biometric templates since 1997.

## IWS BIOMETRIC ENGINE APPLICATIONS

### National Identification Systems

Building a National ID system is no trivial task—it can take months, even years to develop a comprehensive solution that securely issues IDs. The key is to start with a sound enrollment process that verifies the identity of the person to whom the ID is issued. The IWS Biometric Engine can be used to capture a fingerprint, face or other biometric and then search for that individual in a criminal database or "watch list". The same principles can be used to prevent the issuance of duplicate passports, national IDs, and driver licenses, as described earlier.
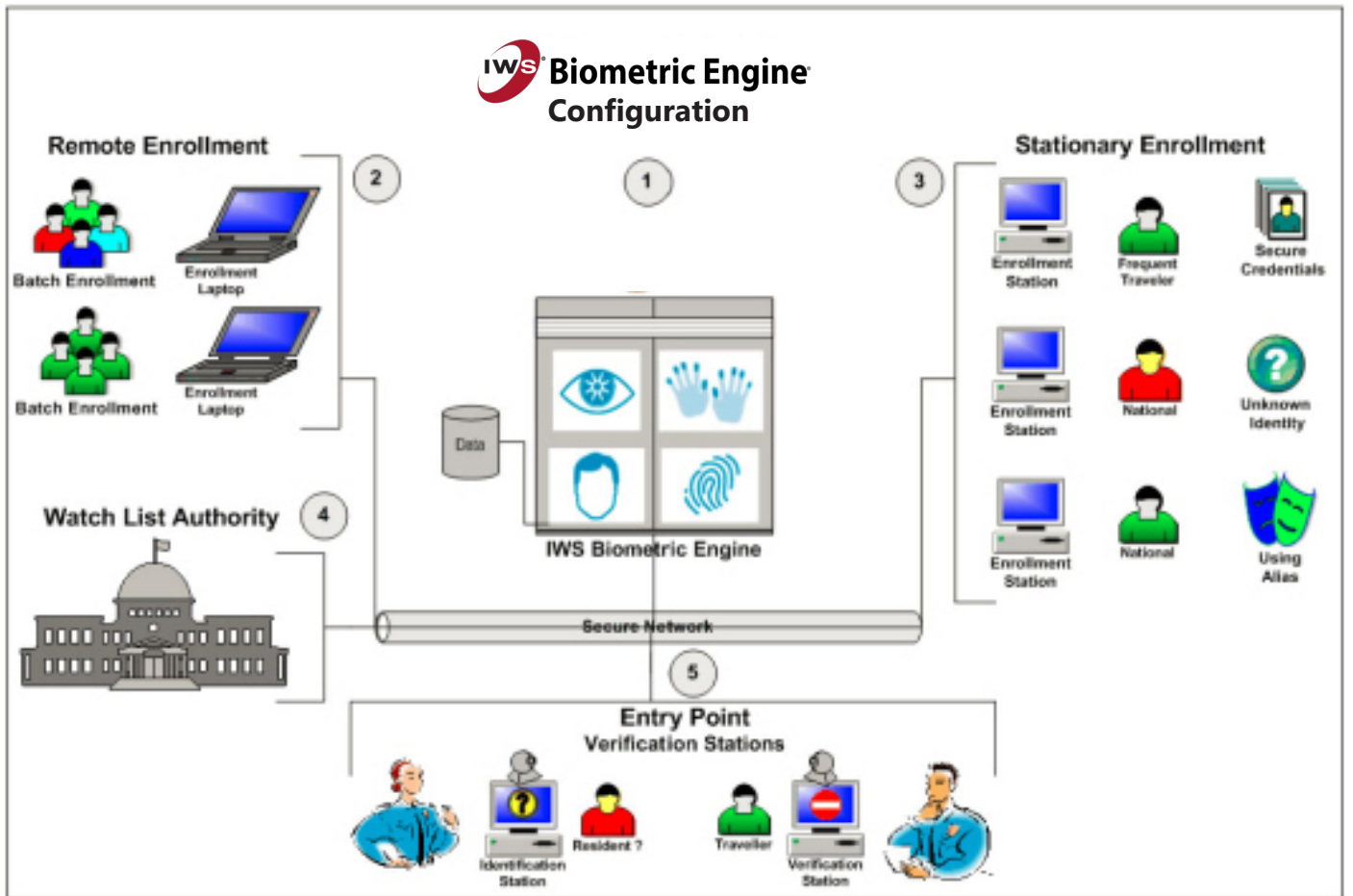
Diagram BE 1

1. IWS Biometric Engine used for Verification, Identification, Watch List, and Duplicate Detection
2. Remote Enrollment Station, can be used for remote locations to enroll populations
3. Stationary Distributed Enrollment Stations placed in Passport Office and Such
4. Watch List Authority such FBI, Interpol
5. Border Entry Locations

IWS Biometric Engine

## Drivers License Systems

A driver license system often involves custom workflow to ensure an ID is issued to the proper person.  In a driver license environment, the IWS Biometric Engine can be used to search the database for duplicate faces and/or fingerprints.  As a result, states can:
- Ensure that the correct individual is assigned the correct license
- Prevent a second license from being issued to an individual using a false name
- Search for multiple identities/aliases

The IWS Biometric Engine can also be used with IWS EPI Builder®. EPI Builder is an SDK used for the development of secure credentials.  By combining EPI Builder and the IWS Biometric Engine, users can develop an integrated driver license system that can capture biometrics and add them to licenses in 2D bar codes or magnetic stripes according to AAMVA (American Association of Motor Vehicle Administrators) encoding standards. For information on EPI Builder, visit www.iwsinc.com.  Because it is SDK-based, the IWS Biometric Engine can also be easily integrated with legacy data systems.

## Airport Security

Knowing the identity of workers and passengers moving through a large, distributed airport facility is a must in today's world.   Workers require secure access to facilities and passengers require security screening before entering waiting areas or boarding flights.

Employees:  Given the disparate employer and employee base in an airport environment, there are a number of significant challenges involved with taking control of employee access rights and badge issuance and management.  The IWS Biometric Engine enables users to enroll an employee whose identity can be authenticated across all participating airports, facilities and applications. Biometric readers simply need to be installed at all principal access points to an airport's physical and electronic assets.  With the IWS Biometric Engine as an integral part of an airport's access control system, security is strengthened and users are given the added benefit of forensic-quality auditing capabilities, all within a common security infrastructure for logical and physical access.

Passengers:  The IWS Biometric Engine supports the entry/exit process as well as loyalty, self-service and registered traveler programs.  With the IWS Biometric Engine, users can enroll a pre-screened traveler who can then bypass long security lines by providing their biometrics (typically a fingerprint or iris scan) at secure points of entry.

## National Border Control Systems

Knowing who is coming into a country is an essential element to national security. The IWS Biometric Engine can be used to capture an individual's biometry such as a fingerprint, face or iris. When combined as part of a national ID and passport/visa issuance system, the IWS Biometric Engine provides a highly secure entry/exit system that verifies the identity of individuals entering or exiting a country.

## Access Control and Facilities Management

Access control is all about keeping unwanted individuals out of a building or a secure facility. There is an increasing need to properly secure and manage physical access systems in a cost efficient way while at the same time securing property, people and access to information. In the past, passwords, PINs, swipe-cards, proximity cards and secure tokens were used to gain entry into secure facilities. Regardless of how widely used these methods are, they can easily be compromised. The IWS Biometric Engine can be used to ensure only individuals with the correct authority gain access to a facility. The IWS Biometric Engine can be used to capture and store a person's biometric data either on a chip embedded in an access control card or central database. When the cardholder approaches the door, he simply needs to verify his identity by running his card through a biometric reader. The biometry on the card or in the database is then compared against the actual biometry of the person trying to gain access. If there is a match, the person is allowed to enter the building, based on his security clearance.

**IWS Biometric Engine can be used to ensure only individuals with the correct authority gain access to a facility.**



**Facial recognition searches can be conducted from scanned and imported images.**

## Voter Identity Verification

An important security feature of any voter registration system is that it needs to prevent an individual from voting more than once. This can be difficult, particularly in countries that don't have the technical infrastructure to support this process. The IWS Biometric Engine enables developers to build biometric enrollment applications using fingerprints, iris scans or any other biometric to populate a national identification registry. Once a national ID program is in place, the IWS Biometric Engine can be used to ensure that each person is uniquely identified before he/she is permitted to vote.

## Law Enforcement Systems

Identifying suspects involved in a crime is no simple task. To aid officers in more quickly identifying potential criminal suspects, IWS provides law enforcement with a digital booking, identification and investigation solution that enables law enforcement organizations to capture, store and retrieve criminal booking data and images. These images include mug shots, fingerprints, scars, marks and tattoos, and can be used to create photo lineups and mug books to help identify suspects involved in a crime and speed the investigative process.

IWS' booking solution includes a facial recognition component that enables users to search the mug shot database for potential suspects whose faces closely match an existing image or a digital composite sketch. Facial recognition searches can be conducted from scanned and imported images as well. This facial recognition component was the first generation version of the IWS Biometric Engine and has been used successfully by ImageWare's law enforcement clients since 1997.

IWS has also recently added livescan capabilities into its digital booking solution providing law enforcement with a second biometric tool to identify criminal suspects. Users can now capture single prints, ten prints or palm prints to further improve the investigative process. In addition, officers no longer need to travel to multiple booking stations to capture fingerprints and mug shots. All booking information, including images, can be located at a central designation and can be routed to the FBI's criminal history record repository.

## ICAO Smart Card Integration

Using the ICAO standards as the guidelines, IWS created a new biometric secure smartcard ID solution using the Oberthur 64K smartcard and the GemBorder 32K smartcard. The person's demographic data, their face, two iris and the full ten fingerprints are enrolled into the Biometric Engine system and an Secure Smartcard as per ICAO current specifications is created. The subjects face, two iris, two fingerprints, and demographic information is encrypted using PKI and stored on the smartcard chip embedded inside the card. The information can only be accessed using the decryption keys and smartcard reader in contact or contactless mode.

The Biometric Engine application is able to perform 1:1 verification using the subject's fingers, face or iris captured in real time and compared against the encrypted information in the ICAO ID smartcard. A person's biometrics can also be captured in real time and compared directly against the Biometric Engine for border control and various other identification usages.

## Amusement and Events

The IWS Biometric Engine can sort through tens of thousands of photographs to find a person of interest in less than a few seconds. When combined with a front-end kiosk, amusement park goers, special event attendees or cruise ship passengers can quickly have a snapshot taken, which can then be used to search for photographs that contain their images, and print them on the spot.

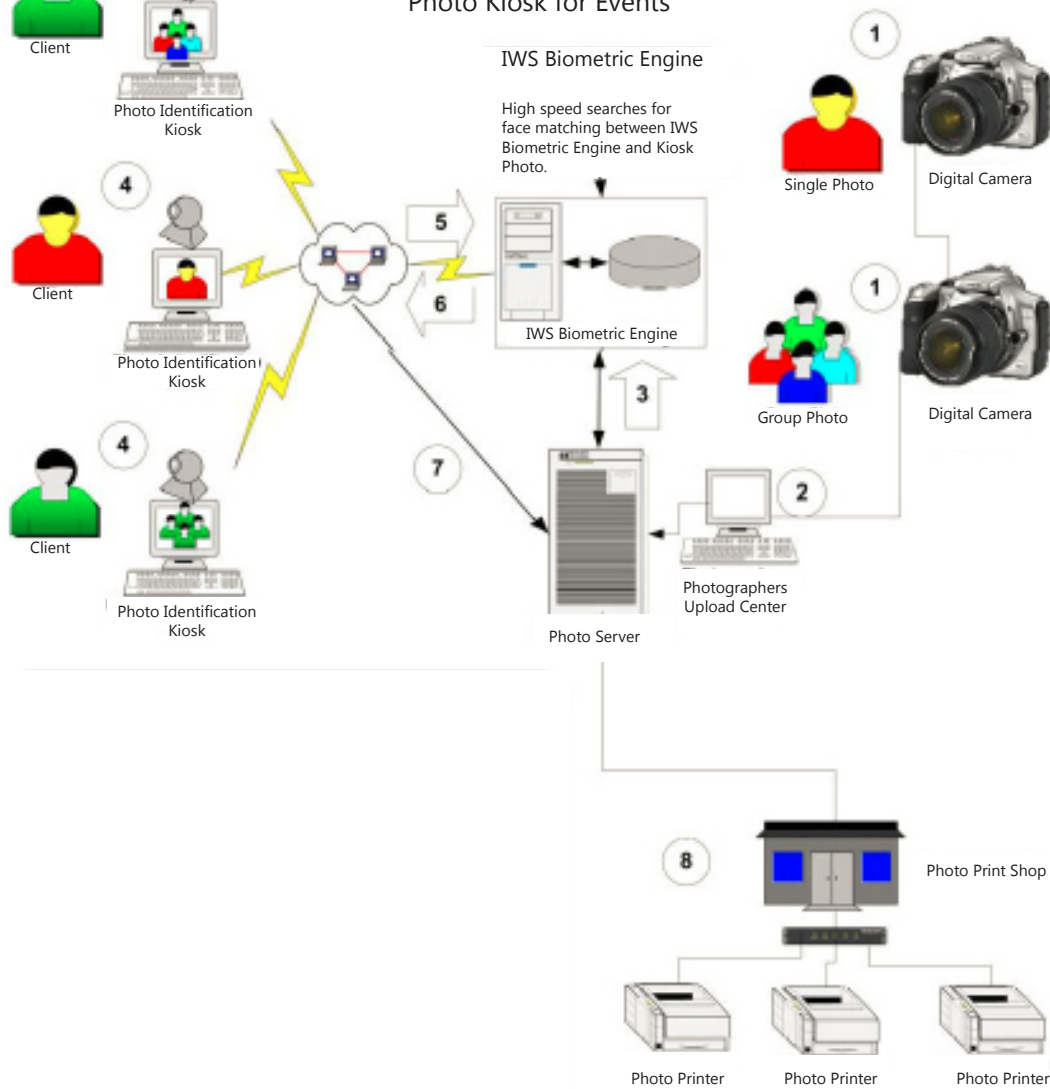Diagram BE 2

## Photos for Amusement and Events

1. Photo is captured by photographer.
2. The images are uploaded to Photo Server in batches.
3. IWS Biometric Engine creates and stores the biometric templates.
4. Clients can go to Photo Kiosk to have their image taken, and their information enrolled into the systems.
5. A biometric template is created from their face and compared to faces in the IWS Biometric Engine Server.
6. If matching images exist they are displayed on the Kiosk computer screen.
7. The client can order the images online from the Kiosk computer.
8. The photos are printed at the Photo Print Shop, where they can be picked up.

## IWS Biometric Engine:

**Easy to Integrate**
**Scalable and Redundant**
**Improves Time to Market**
**Quick Application Process**
**Reduces Testing Time**

### Easy to Integrate

The IWS Biometric Engine's architecture allows developers to quickly add new peripherals and biometrics without rebuilding their applications. An application can even be developed in various compatible development languages where screen customization is a snap. Interfacing with other systems is easy. The IWS Biometric Engine also leverages industry-recognized standards and languages such as BIOAPI, COM, ActiveX, XML and ODBC so programmers and security experts can use familiar development environments. The IWS Biometric Engine also has the ability to run on multiple platforms therefore leveraging the strengths of different operating systems.

### Scalable and Redundant

The IWS Biometric Engine is designed to be scalable and redundant to meet the needs of large organizations. The IWS Biometric Engine achieves scalability by integrating directly into the existing directory service and provisioning infrastructure provided by the underlying network operating system and/or single sign-on platform. Administrators can add additional software components (physical security, application integration, time & attendance) and new hardware devices as the needs of their organizations evolve. The IWS Biometric Engine is architected to manage populations of any size. Search speed and data capacity increase by simply adding off-the-shelf-hardware.

### Improve Time to Market

In today's competitive business environment it's important to leverage existing tools in the marketplace to provide comprehensive and timely biometric solutions. The IWS Biometric Engine allows developers to use familiar tools and easy-to-use components to implement a biometric solution without having to derive biometric functionality from scratch. As a result, the IWS Biometric Engine improves time to market by reducing learning curves and development time.

### Quick Application Process

Biometric requirements change frequently and often in mid-development. Therefore, flexibility is a key requirement. The IWS Biometric Engine's architecture allows developers to quickly plug in biometric devices, new biometric algorithms, enrollment platforms and databases without having to recode the core application. Biometric devices from different vendors can be substituted for one another or the type of biometric can be changed altogether (i.e., swap fingerprint for face). ImageWare's technical team can build custom camera enrollment platforms, integrate biometric devices, build or integrate your application and/or manage a project from start to finish.

### Reduce Testing Time

The reality in today's biometric world is that any large project or application must integrate with a number of biometric acquisition devices, databases and operating systems – each with its own idiosyncrasies. That's why ImageWare has dedicated resources to ensure that the IWS Biometric Engine works with the latest peripherals on the market. For the latest list of products compatible with the IWS Biometric Engine, please refer to the hardware and software compatibility list.
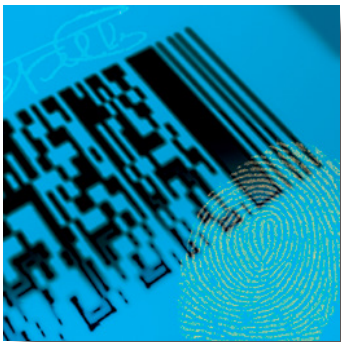
Biometric Engine

## Biometric Algorithms Supported

- Finger - civil
- Finger - livescan
- Face - civil
- Face - NIST-compliant mug shots
- Iris
- Hand Geometry
- Palm - NIST
- Signature
- Voice
- 3D Face

**Note: If a project requires a biometric or peripheral that the IWS Biometric Engine does not support, please contact your ImageWare representative to discuss ImageWare's latest testing efforts and custom offerings.**

- **1:1 Verification** - the process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed
- 1:N Identification - seeking to find an identity amongst a database rather than verify a claimed identity
- **X:N Investigative** - used for watch lists, black lists
- **N:N** – used for duplicate detection at enrollment time
- **Multi-Modal** - using two or more biometric types such as a face and finger search, the modalities are processed through different algorithms and the results are merged together after programmed logic is applied to the results
- **Fusion** - using the same biometric type such as a finger search, the biometric is processed through different algorithms for the same biometric and the results are fused together after programmed logic is applied to the results. Various statistical normalization techniques are used to "correct" the score returned from the results of two biometric searches. Supported Normalization classes consist of:
  - Z-Score
  - Tanh
  - Normal distribution probability
- **Filters** - can be applied to search parameters to focus the search on certain characteristics or demographics

### FIPS 140-2 Level 3

The IWS Biometric Engine was designed to meet the specifications for FIPS 140-2 Level 3, a government standard that aims to maintain the data integrity and security of sensitive information in a cryptographically-enabled system.

FIPS 140 is the Federal Information Processing Standard that outlines security requirements for cryptographic modules. Initially developed for federal agencies using cryptographic-based security systems, the original FIPS 140-2 standard has become a widely used benchmark throughout the business world.

FIPS PUB 140-2 is the Federal Information Processing Standards Publication (FIPS PUB) number 140-2,

"Security Requirements for Cryptographic Modules" - published by NIST (National Institute of Standards and Technology) and copies are available at http://csrc.ncsl.nist.gov/fips/fips140-2/fips1402.pdf

### FIPS 201 (PIV)

Personal Identity Verification (PIV) initiative results from the "Homeland Security Presidential Directive/Hspd-12". The purpose of the PIV, and of its underlying standard (FPIS PUB 201), is to provide a common identification solution for U.S. federal employees and contractors that would permit to achieve a high level of security as well as interoperability across all government agencies. PIV addresses both physical access control to the US government facilities and logical access control to the US government information systems. Fingerprint images are stored as WSQ encoded images encapsulated in an INCIT 381-2004 data record, encapsulated itself in a CBEFF structure.

http://csrc.nist.gov/piv-program

### BioAPI

The BioAPI is intended to provide a high-level generic biometric authentication model; one suited for any form of biometric technology. It covers the basic functions of Enrollment, Verification, and Identification, and includes a database interface to allow a biometric service provider (BSP) to manage the Identification population for optimum

performance. It also provides primitives that allow the application to manage the capture of samples on a client, and the Enrollment, Verification, and Identification on a server. http://www.bioapi.org

## Biometric Application Program Interface (BAPI)

BAPI specifications were designed to be integrated as the lower level of the BioAPI specification.

## Common Biometric Exchange File Format (CBEFF)

CBEFF describes a set of data elements necessary to support biometric technologies in a common way and facilitates biometric data interchange between different system components or between systems. CBEFF also promotes interoperability of biometric-based application programs and systems and provides forward compatibility for technology improvements while simplifying the software and hardware integration process. http://www.itl.nist.gov/div895/isis/bc/cbeff/

## The FBI Fingerprint Image Compression Standard

The significance of this standard was to design and implement a national standard for coding and compression of digitized fingerprint images compressed by the Wavelet Scalar Quantization (WSQ) method.

## Public Key Infrastructure (PKI)

The IWS Biometric Engine uses digital signatures, encryption and decryption (data scrambling and unscrambling) technologies and a comprehensive framework of policies and procedures. A PKI:
- Protects privacy by ensuring that electronic communications cannot be read by unauthorized persons
- Assures the integrity of electronic communications by ensuring that they are not altered during transmission
- Verifies the identity of the parties involved in an electronic transmission
- Ensures that no party involved in an electronic transaction can deny his or her involvement in the transaction

A PKI delivers these assurances through a simple mouse click in a process transparent to the user.

## RSA

RSA is a public-key cryptosystem for both encryption and authentication.

## SSL128

SSL128 (Secure Socket Layer) Handshake Protocol maintains the security and integrity of the transmission channel by using encryption, authentication and message authentication codes.

## Crypto Ciphers:

The IWS Biometric Engine allows the following Administrative Configurable Crypto Ciphers:
- AES
- Triple-DES
- Blowfish

**The IWS Biometric Engine uses digital signatures, encryption and decryption technologies.**

## Biometric Login

User biometrics such as fingerprints or iris scans are required for login.

## Alarms

Alarms such as an email, phone or page can be triggered in the event of various actions such as: three invalid login attempts, security breaches, watch-list hits, black list hits, server failure and system capacity, to name a few.

## Stored Data

Stored data such as images, passwords, demographic data and biometric templates can all be encrypted and stored for system back up, or for re-enrollment of population, to take advantage of new and improved biometric searching algorithms.

## Other Standards

The IWS Biometric Engine is NIST, AAMVA and ICAO compliant:
NIST – National Institute of Standards & Technology, www.nist.gov
AAMVA – American Association of Motor Vehicle Administrators, www.aamva.org
ICAO – International Civil Aviation Organization, www.icao.int

## IWS BIOMETRIC ENGINE COMPONENTS (BASIC COMPONENTS)

## Enrollment

This can be almost any integrated client-side enrollment platform whether it is ImageWare's IWS EPI Builder enrollment module or any other developed platform. The enrollment process is simply to gather the biometric and record information for storage into the IWS Biometric Engine. (1 & 3 in Diagram BE Arc)

## Biometric Engine Router

The Biometric Engine Router handles routing responsibilities including the knowledge of where data is stored and the status of each biometric engine. (2 in Diagram BE Arc)

## Biometric Engine

The biometric engine stores biometric information in memory for instant access. Biometric Engines perform the searches requested by the Biometric Engine Router. The various types of searches that can be performed are 1:1 (verification), 1:N (identification), X:N (watch list), and N:N (duplicate detection). (2 in Diagram BE Arc)

## Verification Stations
The verification station captures an individual's biometrics and uses the IWS Biometric Engine to search the system to verify or identify the individual. The verification station can be a border entry point or an entry point to a secure facility. (1 & 3 in Diagram BE Arc)

## Database

The database stores the same information as the query engine(s). The database is used for system back-ups and various complementary activities, which do not require high-speed searches (such as ID card printing, driver license issuance and passport printing). Original images are kept in the database for the purpose of population re-enrollment to take advantage of new and improved biometric searching algorithms. (4 in Diagram BE Arc)

---

## Standards & Security:
**FIPS 140-2 LEVEL 3**
**FIPS 201 (PIV)**
**BAPI**
**CBEFF**
**FBI Fingerprint Image Compression Standard**
**PKI**
**RSA**
**SSL128**
**Crypto Ciphers**
**Biometric Login**
**Alarms**
**Stored Data**

## Biometric Engine Components:
**Enrollment**
**Biometric Engine Router**
**Biometric Engine**
**Verification Stations**
**Database**
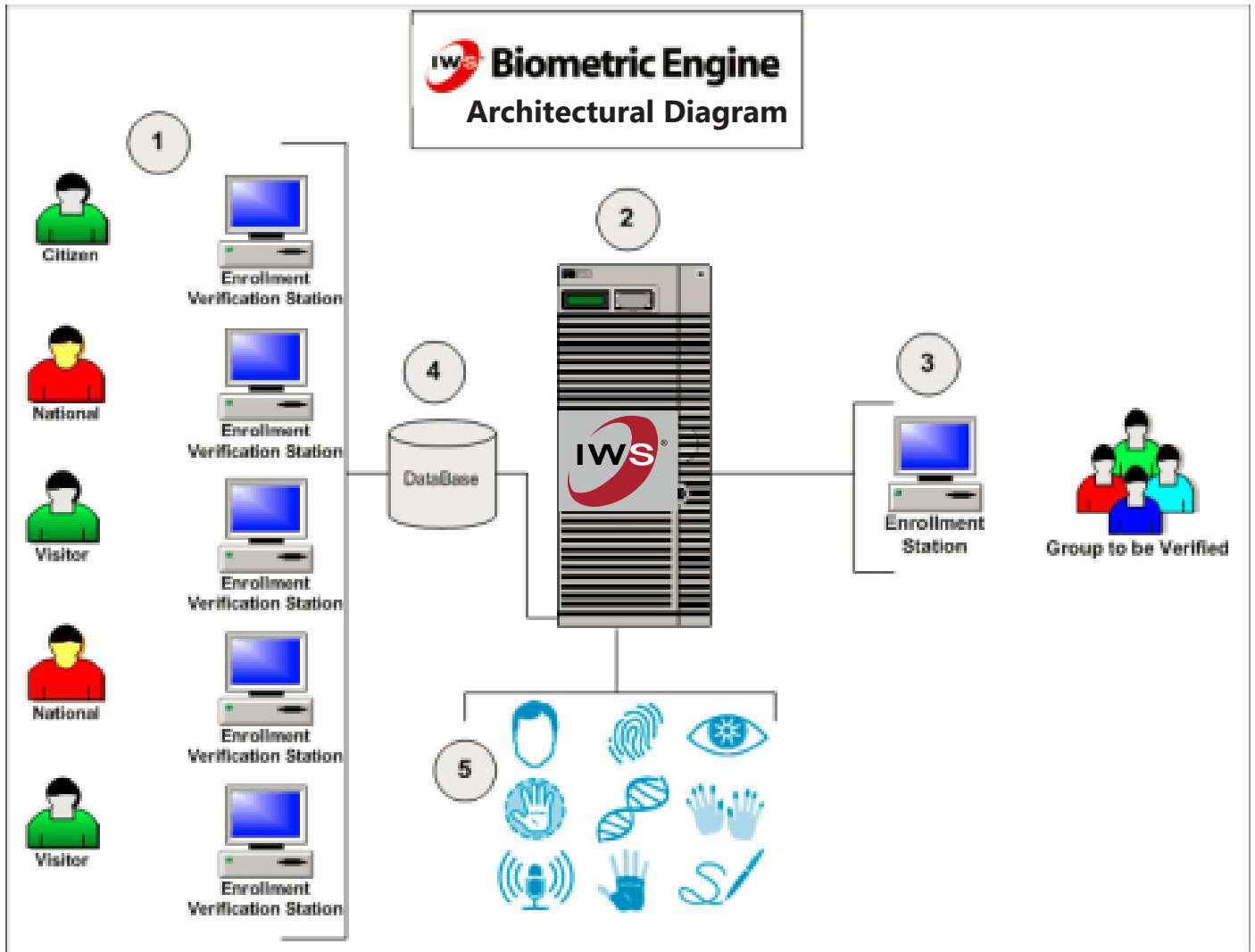**Biometrics**

IWS Biometric Engine®

Diagram BE 1

## Biometric Engine Architectural Diagram

1. Enrollment Station
2. Biometric Engine
3. Verification Station
4. Database
5. Biometrics

## Biometrics

Depending on the requirements, a single biometric or multi-biometrics can be integrated into the IWS Biometric Engine. (5 in Diagram BE Arc)

**IWS BIOMETRIC ENGINE CONFIGURATION**

### High Concurrency

This configuration allows for high concurrency of the Biometric Engine. In this configuration, template records are distributed redundantly to multiple biometric engines so that more than one search can be conducted at any given instant. (1 in Diagram BE Arc)

### High Throughput

This configuration allows for high throughput of the Biometric Engine. A fraction of the template records is distributed to multiple biometric engines, so that each engine need only search through a portion of the entire search set. This allows searches of the entire enrolled population to be conducted in a fraction of the time it would take on a single machine. (3 in Diagram BE Arc)

### High Concurrency & Throughput

This configuration uses both of the above distribution methods and can achieve both very high concurrency and throughput, at the cost of additional hardware.

---

**Biometric Engine Configuration:**

High Concurrency -

Item 1 in Diagram 3


High Throughput -

Item 3 in Diagram 3


High Concurrency &

Throughput

---

## Face (NIST)
- Identix G3, G5, G6\Sagem
- Cognitec
- Viisage
- Neven Vision

## Face (civil)
- Identix G3, G5, G6\Sagem
- Cognitec
- Viisage
- Neven Vision
- Cyber Extruder - SD Face

## Fingerprint (livescan)
- Identix/Sagem
- Bio-Key International
- NEC
- EastShore Technologies
- Lockheed

## Fingerprint (civil)
- Identix/Sagem
- Bio-Key International
- Precise Biometrics
- BioScrypt/Sagem
- Agora
- NEC
- EastShore Technologies

## Iris
- SecuriMetrics
- Iris ID
- Iritech -i-Data Iris SDK 3-X

## Signature
- CIC

## Voice
- Nuance
- IBM
- SpeechPro

## Palm (criminal)
- AFIX Technologies

## Hand Geometry
- Recognition Systems

## 3D Face
- CyberExtruder
- Bioscript/Sagem

## Retina
- Retica

## DNA
- Nuclear
- Mitochondrial

## SUPPORTED BIOMETRIC HARDWARE CAPTURE DEVICES

### Face (civil)
- Canon A/G Series EOS T3
- Logitech Webcam
- Any JPEG

### Face (NIST)
- Sony NTSC
- Canon

### Fingerprint (single)
- CrossMatch Verifier 300/310
- Identix Series/Sagem Morpho
- Precise Biometrics Devices
- Secugen Hamster IV

### Fingerprint (livescan)
- Identix TP3000, TP3800/Sagem
- CrossMatch ID1000, ID500, ID2500
- Any NIST/WSQ Import
- I3 Portable 10 print - Livescan

### Iris
- i-CAM TD-100
- i-CAM 7000 Series
- i-CAM T-10 *pending
- i-CAM D-1000 *pending

### Palm
- Identix/Sagem Morpho
- CrossMatch
- Any NIST Import

### Hand Geometry
- Recognition Systems

### Signature
- ePad-Ink Series
- Any Signature compliant JPEG
- Topaz SigPlus

### Voice
- Any 8bit 16khz microphone
- Any Algorithm compliant WAV

### 3D Face
- Sony NTSC
- Bioscript/Sagem

### Retina
- Retica

### Document Scanner
- Scan1000

## HARDWARE AND SOFTWARE REQUIREMENTS

### Operating Systems
- Microsoft Windows OS (7, 2000 or XP Pro, 2003 Server)
- Unix, Linux for the Server Side

### Databases
- SQL Server 2000
- Oracle 9i
- Oracle 10g
- ODBC 3.0 compliant database management system

### Hardware Servers
- Non Proprietary

### Hardware requirements
- Off-the-shelf blade servers
- Specific hardware configuration and requirements are dependent on the application, desired speed/concurrency and algorithms used

### IWS Biometric Engine Development Environments
Microsoft Visual Basic 6.0
Microsoft Visual C++ 6.0
Miscrosoft ASP 3.0
Microsoft Visual Studio.Net (VB, C++, C Sharpe, ASP)
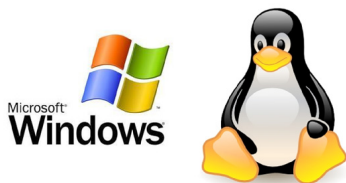
**Biometric Engine**

The IWS Biometric Engine is an SDK-based solution that biometrically manages a group of people of unlimited size and conducts comparative biometric searches. These searches are flexible and can be exhaustive (1:n), specific (1:1) or investigative (x:n). The IWS Biometric Engine is agnostic and is architected to support any type of biometric from any vendor.

The IWS Biometric Engine is based on field-proven ImageWare technology solutions that have been used to manage millions of biometric templates since 1997 and is ideal for a variety of applications including:

- Secure credentials (visa, passport, driver license & national ID)
- Voter identity systems
- Watch lists
- Border control (air, land & sea)
- Airport security systems
- Law enforcement systems
- Amusement and entertainment solutions
- Many smart card biometric applications

The IWS Biometric Engine is scalable, enabling it to manage populations of unlimited size. The IWS Biometric Engine manages biometric images and templates that are enrolled either live or off-line. Because it is vendor independent, the IWS Biometric Engine can support any biometric hardware or algorithm. And because the IWS Biometric Engine stores the enrolled images, a new algorithm can be quickly converted to support new or alternate algorithms and capture devices. The IWS Biometric Engine additionally has a full-featured SDK that allows it to readily integrate with existing applications.

For more information on the IWS Biometric Engine, please contact ImageWare Systems, Inc. at 858-673-8600, sales@iwsinc.com or visit us on the web at www.iwsinc.com.

**10815 Rancho Bernardo Rd., Suite 310
San Diego, CA 92127
p: 858.673.8600
f: 858.673.1770
www.iwsinc.com**

IWS is the leading global developer of identification, biometric and digital imaging software and has been producing secure identity management solutions for over thirteen years. These solutions are currently used by corporate markets, law enforcement, government and transportation, among others, to capture and manage
personal and biometric information and are used for a variety of purposes including:
- Mobile security
- Banking processes
- Criminal booking and watch lists
- Background checks
- Access control
- Identity verification
- Homeland defense
- Secure credentials such as driver licenses and passports
- National ID or medical card programs
- Even professional photography

ImageWare® Systems, Inc. is a proven, patented, multi-modal biometric company with over a decade of providing identity management solutions. Our innovative products such as GoCloudID™ and GoMobile Interactive™ enable extraordinary modular, flexible and scalable identity solutions across a variety of markets including mobile, wireless, financial services and healthcare.

**Biometric Engine®**