

Supported Biometrics.

The IWS Biometric Engine supports multiple biometric algorithms for virtually all leading biometric types including:

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

(Additional biometric types and algorithms will be added as market conditions or users require).

The IWS Biometric Engine is vendor independent; it supports virtually any biometric hardware and algorithm.

Applications.

The IWS Biometric Engine is available as a fully functional Web-based enrollment and identification application or as an SDK that enables it to be integrated into a variety of applications including but not limited to:

- Travel document (visa, passport)
- Border control (air, land & sea)
- Airport security (trusted traveler, employee access)
- Driver license (fraud elimination)
- Watch list
- Voter registration
- National identification
- Time and attendance
- Access control & facilities management
- Background checks (civil & criminal)

Features.

Agnostic

Because the IWS Biometric Engine is vendor independent, it supports virtually any biometric

hardware and algorithm. As a result, organizations are able to leverage existing biometric systems already in place.

Broad searching capabilities

What sets the IWS Biometric Engine apart is the breadth of its comparative searching capabilities. The IWS Biometric Engine conducts searches for:

- Identification of an individual within a population (1:N)
- Identity verification (1:1)
- Investigative searches (X:N)
- Enrollment Integrity searches (N:N)

To provide more accurate results, these searches can:

- Be simultaneous
- Use multiple biometrics (face, finger, iris, etc.)
- Use multiple algorithms of the same biometric type

Additional search features:

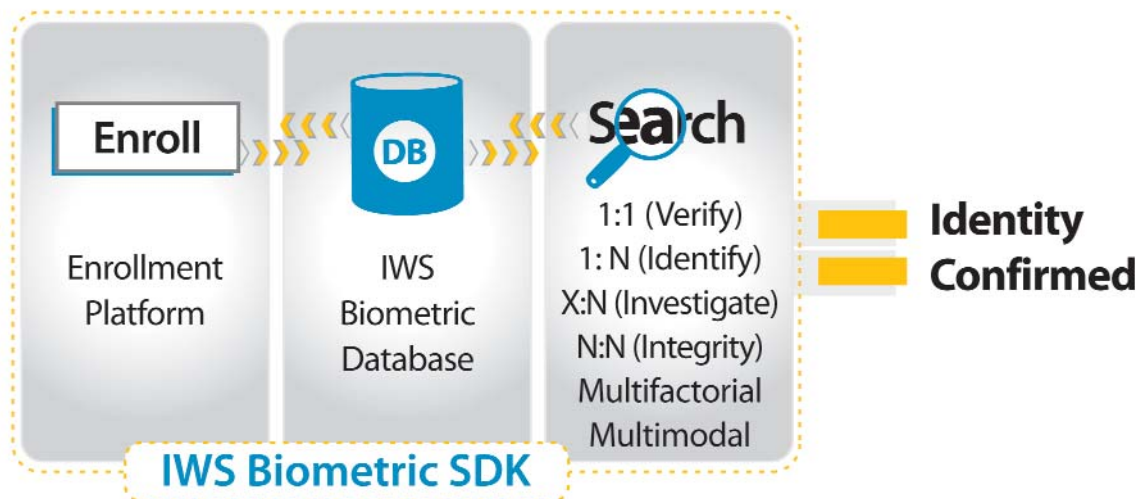
- Search order can be user defined (search face first, then finger)
- Multiple databases can be searched simultaneously
- Filters can be added to narrow searches and speed search time based on demographic data

Easy biometric conversion

Because the IWS Biometric Engine stores enrolled images, not just templates, it can be quickly converted to support additional or alternate biometric algorithms and capture devices to meet evolving market requirements.

SDK-based

As an SDK-based search engine, the IWS Biometric Engine enables developers to imple-



ment a biometric solution or integrate biometric capabilities into existing applications* without having to derive biometric functionality from first principles. The result is a significant savings in development time, costs and resources.

Scalable

The IWS Biometric Engine is scalable, enabling users to store, search and manage populations with an unlimited number of biometric images and templates. Biometric storage capacity and search speed are increased by simply adjusting the server configuration.

Multiple enrollment options

The IWS Biometric Engine offers flexible enrollment options, supporting both live and offline enrollment.

Web applications

The IWS Biometric Engine can be deployed as a Web or Windows-based application.

Secure

Images, passwords, demographic data, biometric images and templates can all be encrypted to ensure the highest security. And the IWS Biometric Engine itself is protected by biometric login capabilities.

*Integrated biometric and secure credential solutions

Combine the IWS Biometric Engine with the IWS™ EPI™ Builder SDK for a comprehensive, integrated biometric and secure credential solution. Designed specifically for high-end ID applications, IWS EPI Builder is used primarily for the production of passports, driver licenses, national IDs, health cards, transit cards and other secure documents.

Benefits.

Reduce learning curves

The IWS Biometric Engine leverages industry-recognized standards and languages such as JAVA, VisualStudio, BioAPI, COM, ActiveX, XML and ODBC, allowing programmers to use familiar development environments, reducing learning curves and development cycles.

Speed time to market

The IWS Biometric Engine allows developers to quickly plug in biometric devices; swap biometric devices from different vendors; change biometric type; and add new biometric algorithms, enrollment platforms and databases without having to recode the core application. As a result, users can address new markets more quickly and speed the overall time to market.

Decrease development time

The IWS Biometric Engine has been tested to ensure it works with current biometric hardware devices on the market today, saving developers significant testing time.

Hardware & Software Compatibility.

Servers

There are no specific server requirements. The IWS Biometric Engine is compatible with readily available, off-the-shelf blade servers. Specific hardware configuration and requirements depend on the application, desired speed and concurrency in addition to the biometric algorithms selected by users.

Capture devices

The IWS Biometric Engine is tested to ensure compatibility with a variety of current market capture devices including multiple:

- Face cameras (live video and NIST-compliant)
- Fingerprint scanners (single and ten print)
- Iris cameras (single and dual eye)
- Signature capture devices
- Hand geometry and palm capture devices
- Document scanners (for offline enrollment)
- Voice capture devices/microphones

Operating systems

- Microsoft Windows 2000, XP Pro or 2003 Server
- Linux (for the server side)

Databases

- SQL Server 2000
- Oracle 9i & 10g
- ODBC 3.0 compliant database management systems

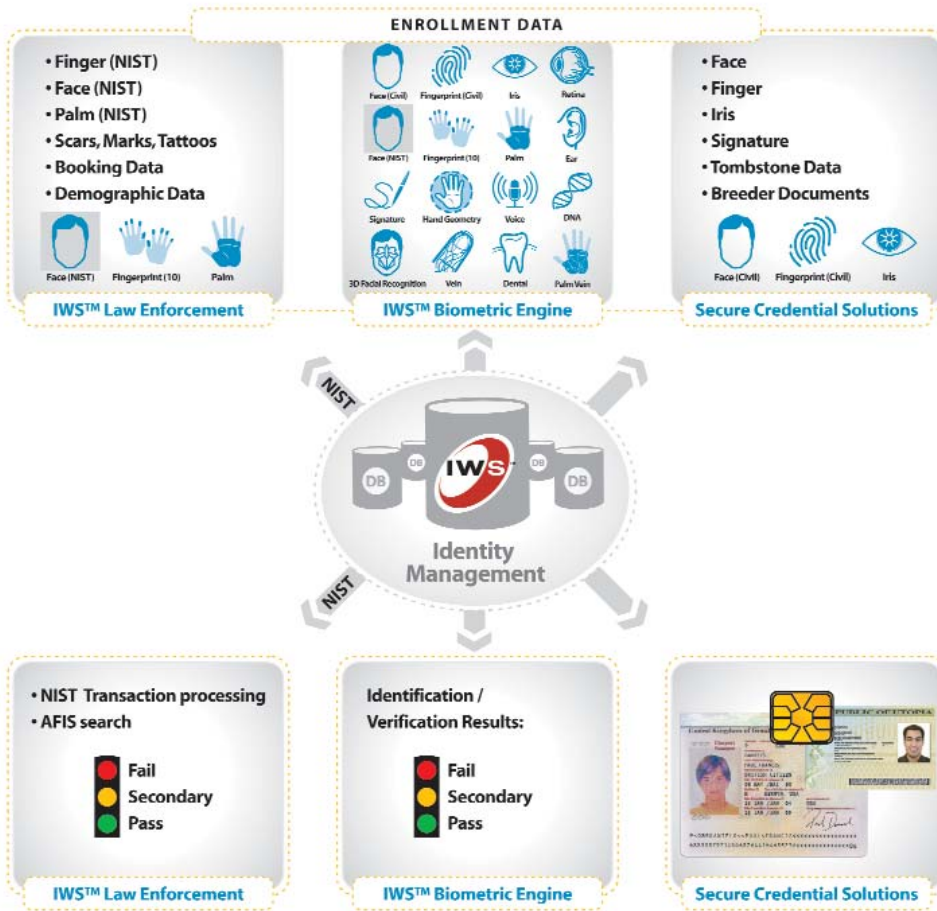
Development Environments.

- Microsoft Visual Basic 6.0
- Microsoft Visual C++ 6.0
- Microsoft ASP 3.0
- Microsoft Visual Studio.Net (VB, C++, C #, ASP)
- Java 1.2

Standards Compliance.

- AAMVA
- ICAO
- NIST
- HSPD-12
- FIPS 140-2 Level 3
- AES FIPS-197
- Triple-DES
- Blowfish
- PKI with RSA
- SSL 128
- X.509
- BioAPI

Identity Management Framework



Contracted by the Mexican Government, ImageWare customized a multi-biometric identification system for Secretaría de Relaciones Exteriores (SRE), the Mexican Ministry of Foreign Affairs. The system, known as SIRLI, incorporates facial, fingerprint, signature and DNA biometric capabilities, and is used to help identify missing and deceased Mexican citizens. The system was developed using ImageWare's Biometric Engine and investigative platforms, enabling SRE to conduct comprehensive biometric and text-based searches of known migrants in the United States and unidentified deceased individuals in U.S. morgues.

The New South Wales Police in Australia leverage IWS' booking, investigative and biometric solutions for law enforcement to create photo lineups and mug books, as well as conduct facial recognition searches on mug shots stored in their IWS digital booking system—all via a secure police WAN / Intranet.

IWS enables the El Hongo prison in Baja California, Mexico to digitally capture, store and search inmate photos, criminal records and related information within a single, centralized database. El Hongo officials also leverage IWS' biometric technology to search these images to identify a list of potential matches based upon distinct facial characteristics.

Sheriff's offices, correction facilities and police departments across the entire State of Arizona use IWS booking and biometric technologies to conduct facial recognition searches on mug shots and civil driver license images. IWS' data sharing capabilities also enable the State to share this data between agencies including the FBI, INS and U.S. Customs.