AWARE

PRODUCT GUIDE

BIOMETRICS SOFTWARE

Mobile Biometric Authentication

Biometric Search and Match SDKs

Fingerprint | Face | Iris

Biometric Enrollment SDKs

Biometric Platforms

Turnkey Solutions

Biometric Applications

Identity Text Analytics

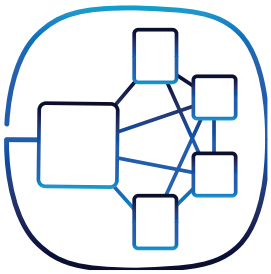
Authentication and Payments ▪ Identity Proofing and Fraud Prevention ▪ Citizen ID and Elections
Visitor Screening and Border Management ▪ Law Enforcement and Investigation ▪ Defense and Intelligence

BIOMETRICS SOFTWARE PRODUCT GUIDE

INTEGRATED SOLUTIONS

Mobile Biometric Authentication Framework

Automated Biometric Identification System



Biometrics as a Service

Browser-based biometric enrollment and data management

BIOMETRIC SUBSYSTEMS

Workflow and Middleware Server

Cluster-Based Biometric Matching Platform

BIOMETRIC MATCHING SDKS

Biometric Search and Match

MINEX Certified (Fingerprint)

BIOMETRIC APPLICATIONS

Multimodal Enrollment (Windows)

Multimodal Enrollment (Android Tablet)

Fingerprint Cards

Forensic Analysis and QA

Application Components (Windows/Browser)

IDENTITY TEXT ANALYTICS SDK

Fuzzy Matching and Identity Resolution

BIOMETRIC ENROLLMENT SDKS

Image Capture and Hardware Abstraction

Data Formatting and Validation

Fingerprint Cards

Image Compression

Mobile Enrollment and Authentication

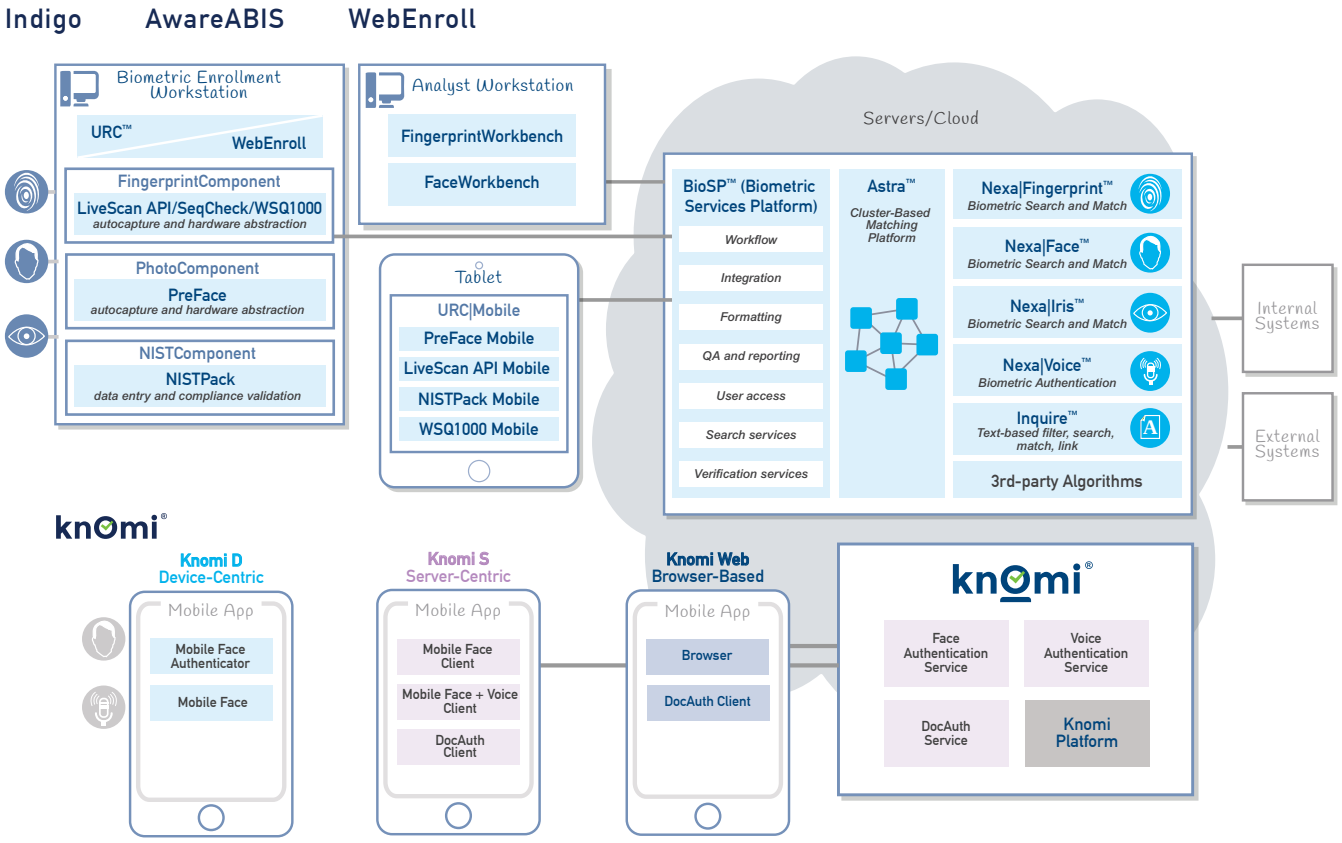
AWARE

www.aware.com | 781-276-4000 | sales@aware.com

Aware, Inc.
40 Middlesex Turnpike, Bedford, MA 01730 USA
T 781.276.4000 F 781.276.4001

www.aware.com

Product Overview



Aware's SDKs, APIs, applications, and subsystems fulfill critical functions within biometric identification and authentication systems. Their modularity and ease-of-integration enable rapid development of customized solutions that are open, flexible, and extensible.

Aware also offers integrated solutions built upon these components to fulfill broader requirements of specific use cases.

Knomi®

Mobile biometric authentication framework

Knomi® is a mobile biometric authentication solution comprised of a family of biometric matching and liveness detection algorithms that use face and voice to enable secure and convenient multifactor authentication without passwords.

Knomi for Mobile Onboarding

Knomi can be used for identity proofing as part of a mobile onboarding solution, with advanced security checks that authenticate driver's licenses and passports, and spoof-resistant biometric facial matching between the live and printed images.

- **Biometric facial match to ID**
- **Document verification**
- **Browser-based capture**
- **Liveness detection**

Knomi for Mobile Authentication

Knomi enables passwordless multifactor authentication using face- and voice-based biometrics and liveness detection. It is available in either a device-centric or server-centric implementation.

- **Multimodal biometrics using NIST-tested face and voice matching algorithms**
- **Device-centric, or server-centric options**
- **Paired with market-leading liveness detection algorithms**
- **Easily configurable for different use cases**

Knomi for Liveness Detection

Knomi's advanced presentation attack detection algorithms are essential for onboarding and authentication. They detect not only victim impersonation spoofs, but also identity concealment spoofs that impact the ability to use the facial images for other biometric identity proofing functions useful for onboarding such as watch list checks and duplicate prevention.

- **Purely passive approach – no user experience impact**
- **Solutions for onboarding, authentication, ID doc verification, kiosks**
- **Device- or server-based architecture**
- **Browser-based option for rapid onboarding**

FEATURES

- **NIST-tested algorithms**
- **Highly configurable UX and security features**
- **Robust presentation attack detection**
- **Multimodal performance**
- **Identity proofing and document authentication**
- **Device- or server-centric architecture IAM integrations**
- **IAM integrations**
- **iOS, Android, Windows, Linux support**

APPLICATIONS

Mobile banking

Banks can incorporate Knomi into their apps to make mobile onboarding and login more secure and convenient for their customers.

Enterprise security

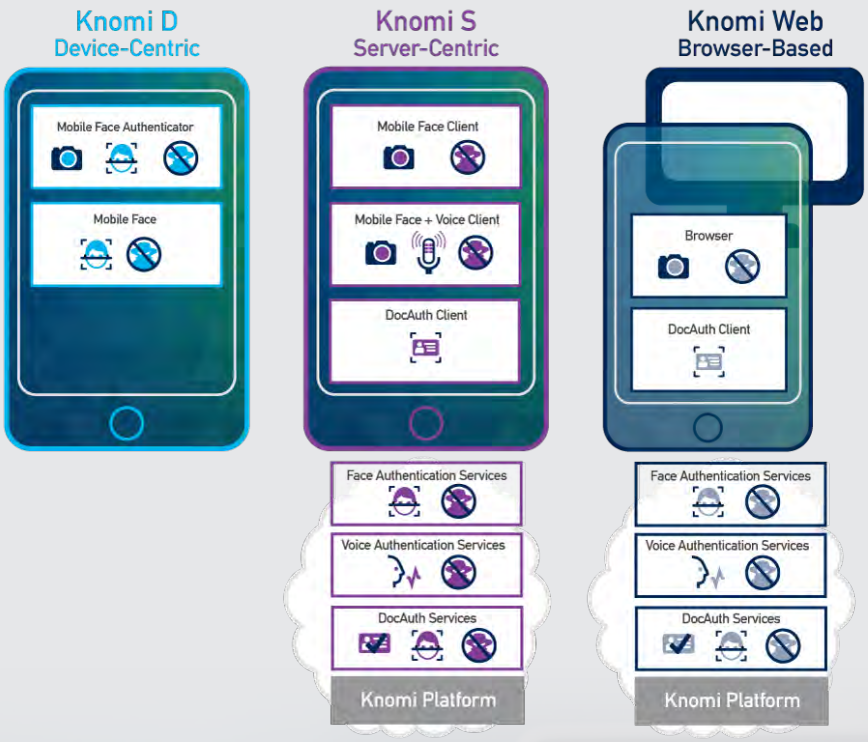
Companies can use Knomi to make access to their digital assets more secure for their workforce.

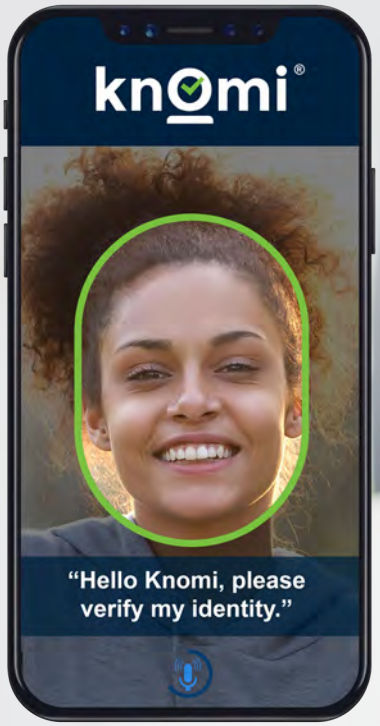
Government

Government agencies can use Knomi to make logical and physical access control more secure for employees and contractors.

Architecture support: device- and server-centric, and browser-based

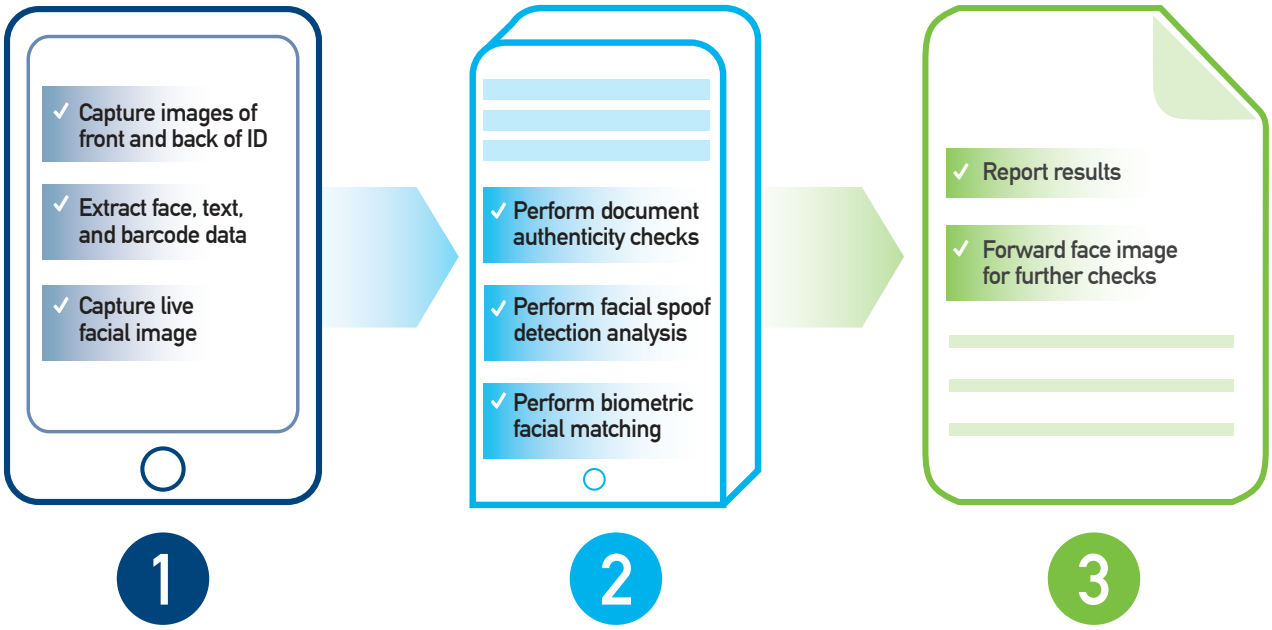
Three architectures are supported: Device-Centric, Server-Centric with Mobile SDK, and Server-Centric with Web. Knomi D offers software that performs all functions on the device. Knomi S moves functions to the server, including biometric template creation, matching and storage. Knomi Web enables facial capture and liveness detection via any browser. Knomi DocAuth can be implemented to support server centric with mobile SDKs and server centric with web architecture.





Knomi DocAuth

Document authentication and facial matching for identity proofing upon mobile onboarding



Knomi includes a solution for document authentication and facial matching, which is ideal for biometric identity proofing as part of a mobile onboarding process using a government-issued credential such as a driver's license or passport. Knomi DocAuth can be implemented in either a device- or server-centric architecture.

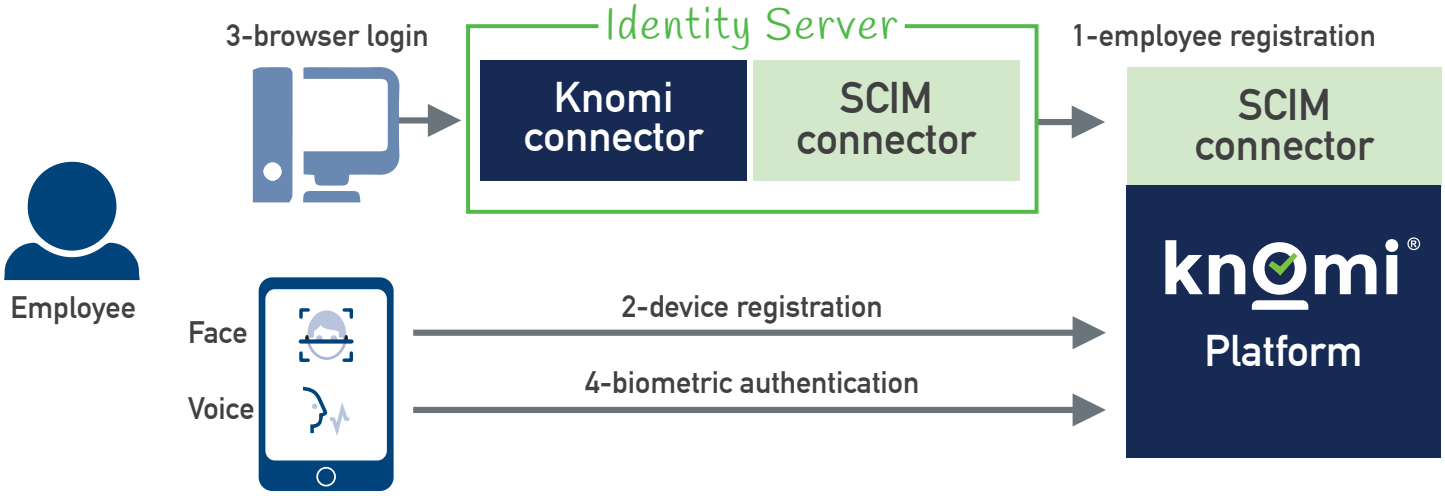
- **Assisted capture of credential (front and back)**
- **OCR-powered capture of printed and bar-encoded data**
- **Detection of document security features (white light)**
- **Automated capture of printed facial image and live facial image**
- **NIST-tested facial recognition algorithms**
- **Robust, multi-algorithm face spoof detection for authentication and identity proofing (paper, digital, video, 2D/3D masks)**
- **Comparison of printed to bar-encoded data**
- **NFC reading of e-passport chip data**
- **Device-or server-centric architecture**

Knomi Platform

Integration with market leading identity and access management platforms

Knomi Platform is the component of the Knomi mobile biometric authentication framework that can be integrated with identity servers to quickly enable them with passwordless multifactor authentication (MFA) using biometrics on a mobile device.

For organizations using an identity and access management (IAM) platform to implement secure access control, SSO, and federation for employees or customers, adding Knomi enables users to login to assets normally accessible by PC or browser with a username and password by instead biometrically authenticating on their mobile device in passwordless fashion. Knomi Platform has been integrated with several leading identity and access management products. Any enterprise can integrate Knomi to enhance their identity platform with passwordless multifactor authentication using out-of-band mobile biometrics, making login to their online assets more secure and convenient for their employees.



Out of band multifactor authentication using mobile biometrics

Knomi® - Liveness Detection

Face and voice liveness detection for biometrics-enabled mobile onboarding and authentication

Biometrics make mobile onboarding and authentication more convenient and secure, but liveness detection is essential for biometric applications where security is paramount and fraud is a risk. Liveness detection assures the integrity of a variety of biometric security checks, including mobile authentication, document verification, and watch list search. Knomi provides the best-performing device-independent liveness solution available that is truly passive, with an opaque user experience that does not instruct a fraudster how it might be defeated.

The Knomi mobile biometric authentication framework offers high-performance, field-proven face and voice liveness detection, with a family of machine learning-based algorithms that detect and prevent virtually all types of biometric presentation attacks. Knomi detects attacks attempting victim impersonation as well as those attempting identity concealment, which is especially important for onboarding. Knomi's face liveness algorithms detect obstructions and distortions, and work in low-light and bright-light conditions on all types of faces.

Voice authentication and liveness can be optionally be added and fused with face to make spoofing exponentially more difficult for fraudsters. Knomi detects a variety of voice spoof types, including recorded, filtered, and synthetic voice spoofs.

Knomi SDKs and APIs can be incorporated into either a mobile-, browser-, or kiosk-based application. It can be implemented with a server-, or device-based architecture (with, **Knomi S**, or **Knomi D**, respectively). Server-based Knomi Web enables face capture and liveness detection from a browser on a mobile device or desktop.

FEATURES

- **Liveness detection algorithms and workflows optimized for onboarding, mobile authentication, document verification, and kiosk-based solutions**
- **Purely passive, machine learning-based approach, with no user friction**
- **Opaque user experience that avoids training fraudsters how to defeat it**
- **Device- or server-based implementation alternatives**
- **Configurable workflows and performance thresholds**
- **Easy integration using on-device SDKs, server-based APIs, and reference UI code**
- **Browser-based capture mode works on mobiles and desktops**
- **A la carte purchase options, with liveness, matching, face, and voice offered independently**
- **Server-based option that works across devices without multiple enrollments**
- **iOS and Android mobile versions; Windows and Linux server versions**
- **Comprehensive technical support**

USE CASES AND OPTIONS

	Mobile app	Mobile browser	Desktop browser	Kiosk
Onboarding	✓	✓	✓	
with document verification	✓	✓		
with biometric search	✓	✓	✓	✓
Biometric authentication	✓	✓*		✓
				✓

* In support of mobile out-of-band authentication

ATTACK TYPES DETECTED

Victim impersonation

- **Fraudster attempts to defeat a security mechanism by impersonating a victim with a biometrically matching spoof**

Identity concealment

- **Fraudster attempts to conceal their identity to avoid detection in biometric searches and eliminate evidence of their activity**

ATTACK DETECTION FEATURES

Face

- **Detection of**
  - **Digital photos and videos**
  - **Paper photos and masks**
  - **High-quality 3D masks**
  - **Partial obstructions and distortions**
- **Low-light and bright-light conditions**
- **Wide range of face types**
- **Optional fusion with voice**

Voice

- **Detection of**
  - **Recorded voice**
  - **Modulated voice**
  - **Filtered voice**
  - **Synthetic voice**
- **Optional fusion with face**

AwareABIS™ - The open ABIS

Modular architecture, rich web services, user-configurable workflows, unfettered data access, algorithm choice

AwareABIS™ is an Automated Biometric Identification System (ABIS) used for large-scale biometric identification and deduplication, with support for fingerprint, face, and iris modalities. Its highly modular architecture allows it to be configured and optimized for either civil or criminal applications.

AwareABIS leverages BioSP™ (Biometric Services Platform), Aware's market-leading workflow and integration server to achieve unsurpassed configurability and ease-of-integration. It has the flexibility to utilize Aware's high-performance, NIST-tested Nexa™ face, fingerprint, and iris matching algorithms, as well as top-tier fingerprint algorithms from 3rd-party providers. Together, these features make it the best ABIS on the market not only for extreme configurability but for prevention of vendor lock-in.

AwareABIS is also fast, scalable, and reliable, using Astra™, an advanced cluster computing platform to perform searches against millions or tens-of-millions of records.

APPLICATIONS

- Fingerprint-based search (AFIS)
- Biometric deduplication
- Civil identity proofing
- National ID
- Border management

FEATURES

- Extreme configurability
- Top-tier fingerprint matching performance
- Multimodal support
- Browser-based interfaces
- Rich web services
- Hyper-scalability
- High availability and fault-tolerant
- Unlimited data access
- Support for 3rd-party algorithms

Configured as a **civil ABIS**, AwareABIS provides powerful biometric search capability through open APIs that are well-designed and easy to use. Aware's powerful client applications are offered to provide powerful front-end capabilities, or custom applications can be used to fulfill project-specific requirements.

Configured as a **criminal ABIS**, AwareABIS provides all the useful features of the civil ABIS and adds powerful capabilities critical to law enforcement applications, such as comprehensive analysis, processing, and search of both latents and facial photographs.

CRIMINAL ABIS FEATURES

Comprehensive latent fingerprint search support

Comprehensive support for latent examination, processing, latent-live and latent-latent matching

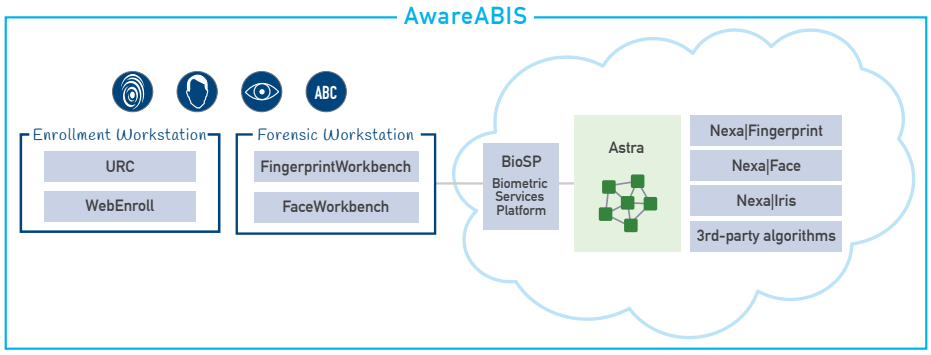
Modern fingerprint and face examiner applications

Matcher-agnostic forensic face and fingerprint workstation applications, designed by examiners to offer a rich analytics feature set, useful workflow tools, and excellent reporting capability

Market-leading data formatting and validation

Incorporates Aware's NISTPack™, the industry standard for ANSI NIST/EBTS biometric data file formatting, validation, and interchange

AwareABIS™ is built upon several mature, high-performance, field-proven applications, platforms, and algorithms from Aware. Components are available a la carte depending on the application and system requirements. It is also compatible with 3rd party biometric matching algorithms.



Workflow configurability, ease-of-integration, and powerful onboard processing

BioSP™ is a service-oriented platform used to enable a biometric system with advanced biometric data processing and management functionality in a web services architecture. It is feature-rich and highly configurable, providing programmable workflow, data management and formatting, and other important utilities useful in large-scale integrated biometric systems. BioSP Workflow Manager allows stateful processing workflows that involves user interaction, such as approvals, reviews, or edits. The workflow is scripted using BPEL, which allows it to be easily modified to many use cases. Each state of the workflow can have a different owner, and history is tracked over the lifecycle.

BioSP offers powerful software modules and a rich array of web-based services, including messaging, submissions, responses, and logging. They enable AwareABIS with valuable features that are easy to integrate with external systems.

BioSP Subject Manager provides services for managing and archiving subject identity data, both biographic and biometric, as well as custom metadata. Subject Manager manages the server side of biometric enrollment processes, the collection of biometric samples (images or templates) and biographic data for credentialing, biometric identification, or biometric verification. It provides support for finger, face, palm, iris, and scar/mark/tattoo images.

BioSP Transaction Manager provides services for building transaction workflows between multiple disparate systems, including enrollment clients and other back-end systems. It is driven by BPEL workflow definitions and is highly configurable, managing both receipt of submissions and processing of responses from distributed sources. Store-and-forward requirements for standards-based communication with local, state, federal, and international government agencies are addressed with Transaction Manager.

BioSP Format Manager provides s ervices for working with various open standards data formats to enable interchange of biometric and biographic data. Format Manager parses, validates, constructs or transcodes standard-compliant biometric data structures, including those formats defined by ANSI/NIST, ANSI/INCITS, ISO/IEC, FIPS-201, and ICAO.

Fast, scalable, and reliable

AwareABIS utilizes Astra, a distributed cluster computing framework that is field-proven, reliable, and well-supported. It is highly fault-tolerant with integrated failover capability, and includes a browser-based system monitoring dashboard that allows administrators to know the performance of the system at all times and be alerted when problems arise.

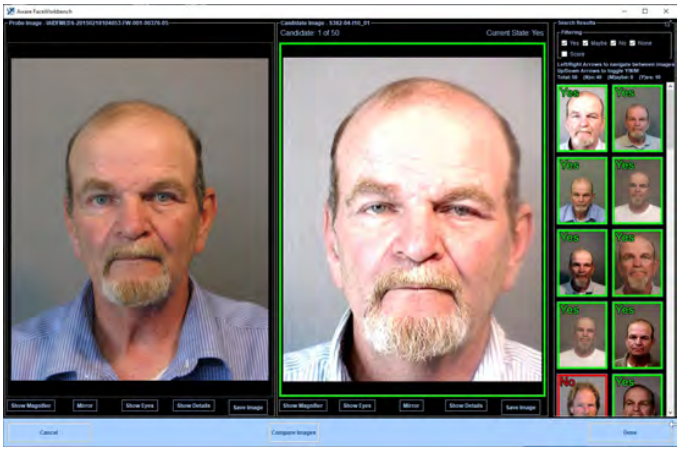
AwareABIS configures a multi-node computing topology and deploys the algorithms and data for fingerprint, face, and iris recognition to each node, then manages the execution of the millions of operations and results in such a way that maximizes the utilization of the machines and processors. The platform is independent of the algorithms in use, so long as access to 1:1 matching capability of the algorithm is provided. The platform can run one or more biometric and text matching algorithms in either staged or parallel search configurations.

AwareABIS provides system configuration, management, and monitoring. System topology and workflows are configured. The biometric data cache is managed. Biometric matching algorithms are configured, managed and deployed. A browser-based system monitoring dashboard provides alerts and statistical information about the operation of the system. The cluster controller executes commands and computations across multiple computing nodes. It deploys biometric and text matching algorithms and data to each node.

COMPREHENSIVE FINGERPRINT AND FACE EXAMINATION WORKSTATIONS

FaceWorkbench™

FaceWorkbench is a client application used by biometric examiners to perform facial reviews in various biometric operation workflows, including 1:N, 1:1, and training. It is distinguished by its thoughtful and forward-looking incorporation of current and emerging guidelines and best practices resulting from recent work in the forensic community within the US Government, international standards bodies, and independent forensic associations.



Search results view

FaceWorkbench integrates examination-based workflows for comparison and training enabling a facial examiner to work in the most efficient way possible while enforcing these current and emerging guidelines and best practices in a supportive role. FaceWorkbench also incorporates numerous ease-of-use features for the facial examiner so critical tools and resources needed for an examination are readily available and effective to use with minimal effort.

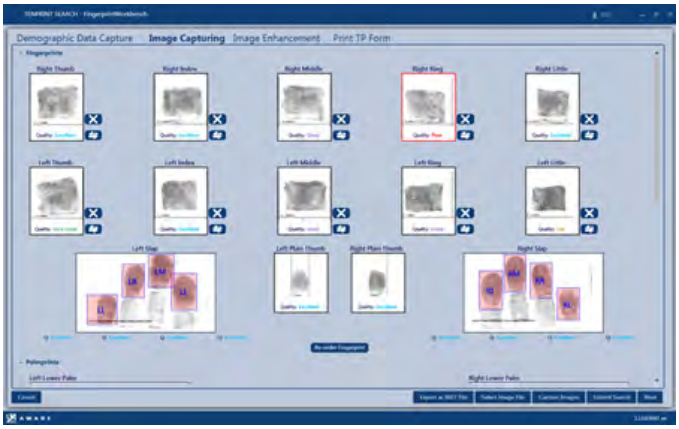
FEATURES

- **Single or bulk facial match submissions**
- **Comprehensive examination workflow in one cohesive application**
  - **queue management**
  - **image calibration**
  - **intense 1:1 review**
  - **reporting**

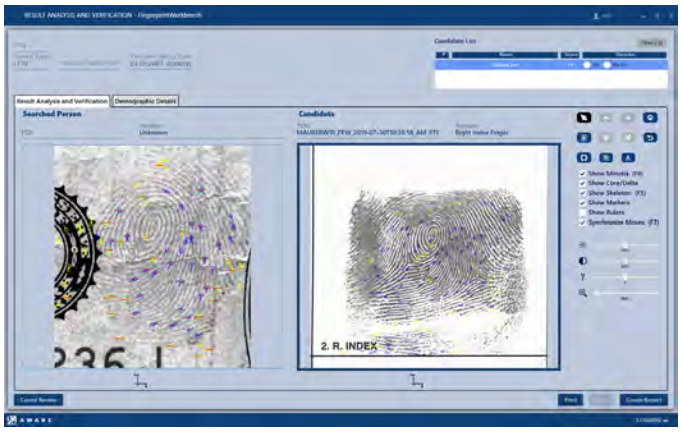
- **Reduces or eliminates tedious processes**
- **Provides useful image analysis features**
- **Instant access to operational guideline documents**
- **In-application reporting**
- **Integrated training mode**
- **Easy screen capture and terminology references**
- **Automated report generation**

FINGERPRINTWORKBENCH™

FingerprintWorkbench is a workstation application used by fingerprint examiners to perform latent fingerprint examination and tenprint match results review and reporting. Used as part of AwareABIS, it provides useful, intuitive tools and workflows that help the examiner to complete their tasks more effectively and more efficiently, with support for 1:1 comparison and 1:many search.



Tenprint search



Latent search results analysis and verification

Distinguished by its forward-looking, intuitive design and comprehensive capability set, FingerprintWorkbench offers workflows highly optimized for efficiency and high performance as well as configurable input (live scan and card scan format options) and output (print card format). It does so in part by incorporating useful examination tools–readily available with minimal effort–directly into the workflows, while also enforcing best practices.

FEATURES

- **Comprehensive search workflows**
  – Tenprint to tenprint or latent
  – Latent to tenprint, palm, or latent
- **Livescan, print card, file image, and biographics submission**
- **Management of search queues**
- **Appendix F certified card scanning, formatting, output**
- **Several supported workflows**
  – Latent and tenprint registration
  – Queue management
  – Latent match charting
  – Decision verification
- **Image processing features**
  – Histogram (brightness, contrast, equalization, etc.)
  – Sharpness
  – Ghost removal
- **Minutiae processing**
  – Add/delete
  – Quality filtering
- **Match results verification**
  – Minutiae pair mating
  – Annotation of final decision
- **Latent match charting**
  – Assists in courtroom presentation of match results

Powerful matchers from Aware or 3rd parties

AwareABIS can be equipped with Aware's NIST-tested Nexa|Fingerprint™, Nexa|Face™, and Nexa|Iris™ algorithms for biometric search using fingerprint, facial, and iris. Multiple modalities can be fused for substantially improved performance.

Unlike other ABIS, AwareABIS™ can utilize biometric algorithms from other suppliers.

Indigo™

Biometrics as a service

Indigo™ is Aware's family of cloud-based biometric APIs and turnkey solutions, each provided as a subscription-based software-as-a-service (SaaS).

Indigo|API provides biometric face and fingerprint image analysis, matching, and enrollment functionality; all as granular REST services that can be easily incorporated and orchestrated to enhance identity systems with powerful, high-performance biometric functionality. These functions include quality scoring, liveness detection, enrollment, verify, compare, and search for fingerprint and face modalities.

Indigo turnkey solutions deliver powerful biometric capabilities accessible from a browser on a subscription basis. Each Indigo solution is specifically designed for a particular use case:

- **biometric identity proofing for onboarding of new customers and employees**
- **kiosk-based biometric patient identification**
- **mobile time and attendance using biometric authentication to validate time and location data**

Worklist display, with alert showing duplicate record found; potential fraud or error

Users of Indigo "biometrics-as-as-service" gain the traditional benefits associated with SaaS; namely the lower costs and risks of a "pay as you grow" subscription model as compared to upfront license fees. All Indigo offerings are built upon Aware's time-tested, market-leading software components for biometric enrollment, analysis, and matching.

FEATURES

Cloud-based SaaS

Offered as a software-as-a-service (SaaS) subscription.

Turnkey capability

Integration is possible but not required to gain powerful functionality from Indigo.

Mature technology

Built upon Aware's market-leading BioSP™ (Biometric Services Platform), and/or biometric algorithm products.

Fully scalable fingerprint and face search

Enables rapid, high-volume processing and search of of face and fingerprint records.

Role-based access control

Certain privileges can be reserved for credentialed administrators, and restricted from operations specialists.

Rich administrative features

Includes capabilities that help users configure the system, view and edit data, set access rights, and generate reports.

APPLICATIONS

Applicant onboarding

Confidently assess whether a prospective customer or employee has been previously encountered.

Patient identification

Use biometrics to avoid duplicate identity records and misidentification of patients.

Time and attendance

Use mobile devices to collect time and location data that is validated using biometric authentication.

Fraud detection and deterrence

Deter and detect fraud by ensuring that applicants cannot misrepresent their identity, either now or in the future.

Duplicate and error prevention

Prevent duplicate identity records in an identity management system using the unique power of biometrics.

Watch list search

Detect whether individuals have been previously cited as a person of concern.

Mobile biometric authentication

Use Indigo|API web services to incorporate face and voice biometric matching and liveness detection into your mobile authentication solution.

Liveness detection

Use Indigo|API web services to determine whether biometric face and voice are live or spoof attempts.

Biometric sample processing

Perform analysis, quality scoring, and optimization of biometric fingerprint and face images.

Indigo|API™

Indigo|API is a family of cloud-based REST services that can be used to perform granular biometric analysis and processing functions for face and fingerprint images. These include quality, liveness, enroll, verify, compare, and search for fingerprint and face biometrics.

FINGERPRINT

- Quality Check
- Compare
- Enroll
- Verify
- Search

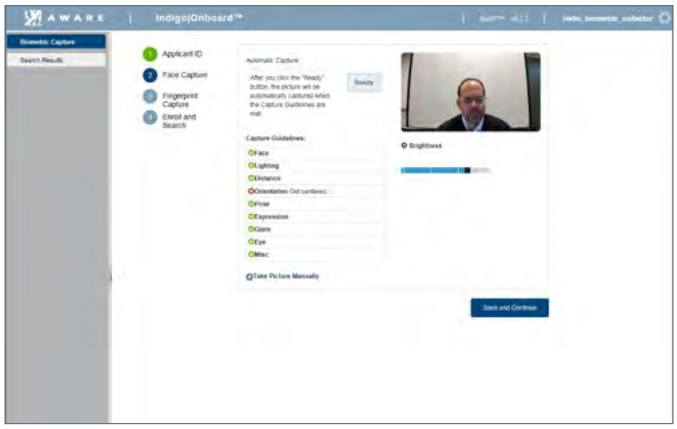
FACE

- Quality Check
- Liveness
- Compare
- Enroll
- Verify
- Search

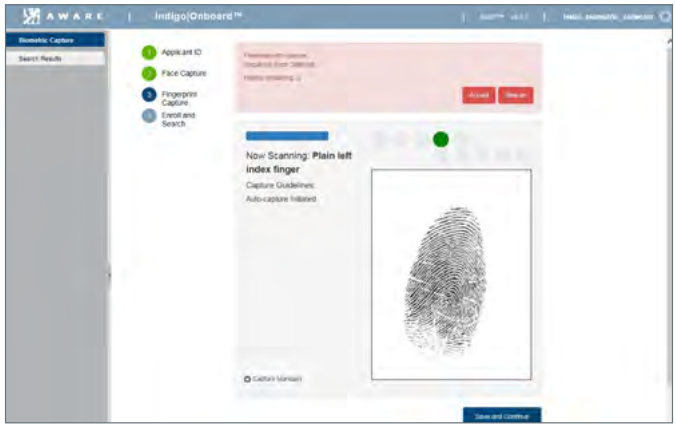
Indigo for Onboarding

Indigo leverages biometrics to enhance the onboarding process with a fast and confident determination of whether someone has an existing identity record in the system. In this way, attempts at identity fraud can be detected and duplicate identity records prevented.

Indigo provides browser-based capture of fingerprints and faces and scalable one-to-many search of millions of records. It separates the enrollment and investigation processes into two asynchronous steps so they can be performed and administered by personnel with different skills and credentials. Fingerprint data is searched against all records previously enrolled in the system, and positive search results are queued in a worklist as alerts that include the associated facial images. As a separate asynchronous process, alerts are used to prompt further investigation and then to either close or escalate the case.



Autocapture of facial image with real-time image quality assurance and camera integration

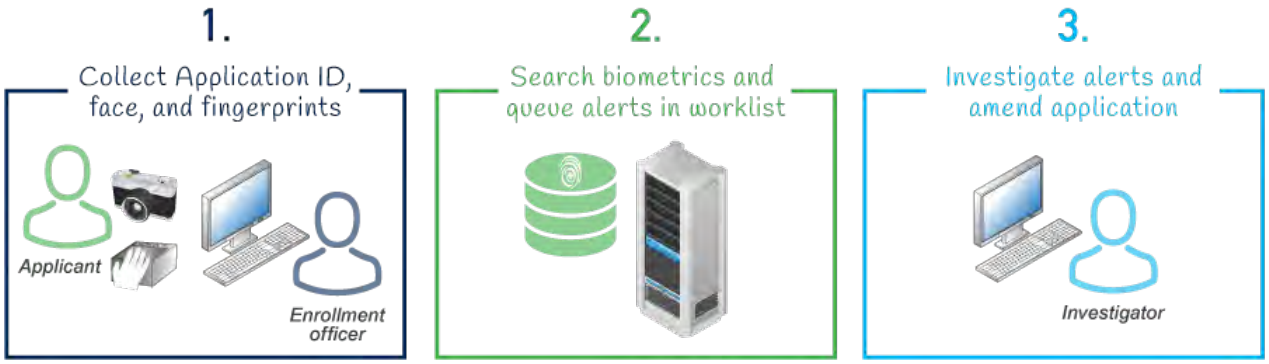


Fingerprint autocapture with error detection and device integration

FEATURES

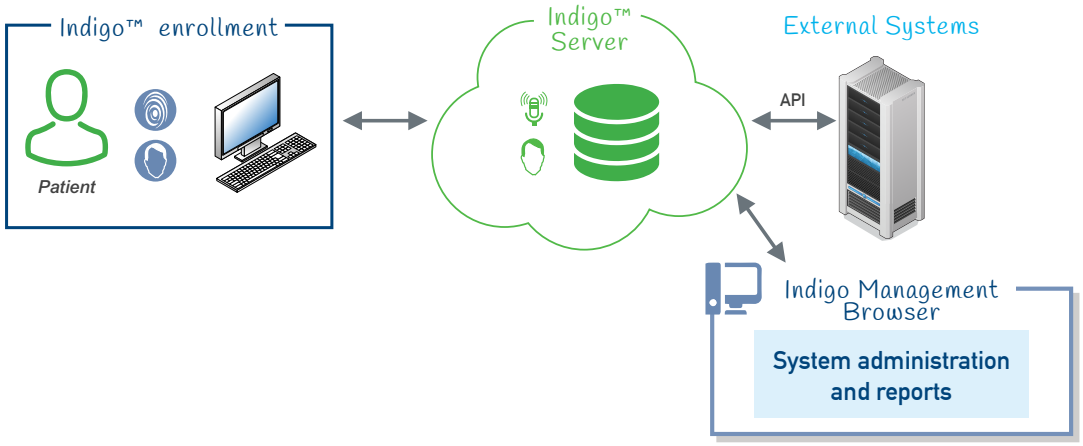
- **Software-as-a-service or private cloud**
- **No system integration required**
- **Web-based fingerprint and face enrollment**
- **Highly scalable fingerprint search**
- **Separation of enrollment and review tasks**
- **Role-based task assignment and data access**
- **Mature, field-proven platform**

- **Software-as-a-service or private cloud**
- **No system integration required**
- **Web-based fingerprint and face enrollment**
- **Highly scalable fingerprint search**
- **Separation of enrollment and review tasks**
- **Role-based task assignment and data access**
- **Mature, field-proven platform**



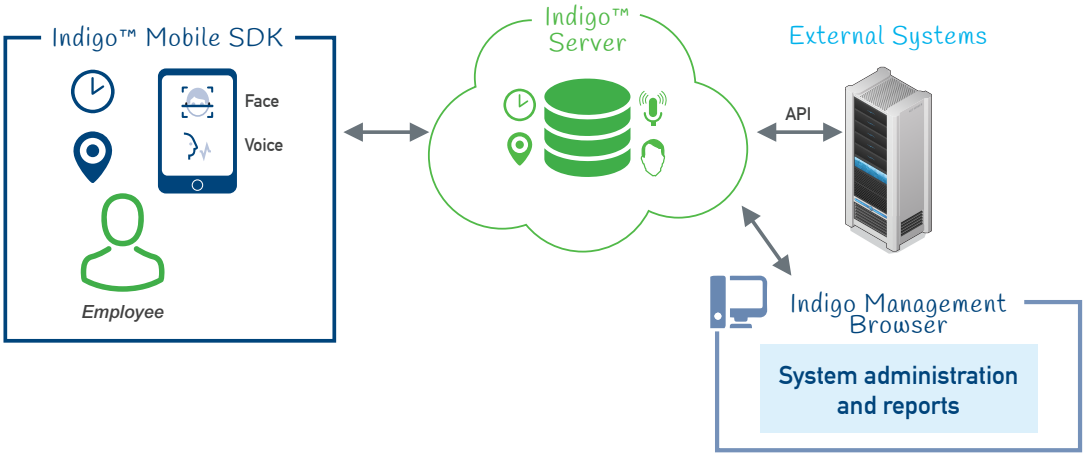
Indigo for Patient Identification

Indigo provides an easy and effective way to identify patients when they arrive to receive care. It is kiosk based, with patients able to self-enroll. It can be integrated into existing applications and workflow. A patient simply submits their biometric data, which initiates a biometric search, the results of which are reported via API to a system of choice. Workflows can be configured to automate processes based on whether the patient is identified as new or existing.



Indigo for Time & Attendance

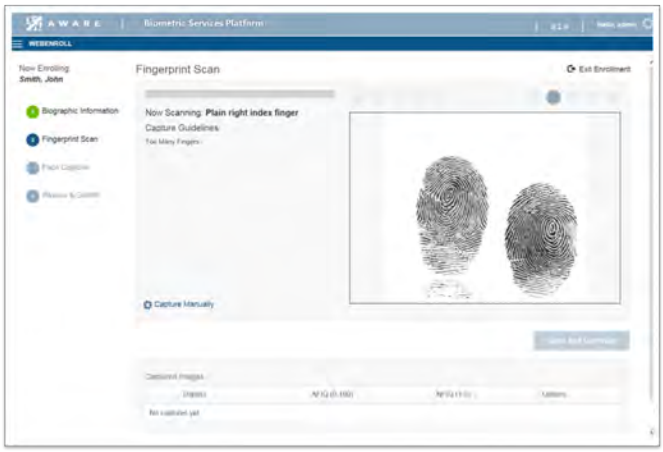
Indigo can be configured as a mobile biometric time and attendance solution e that uses a mobile device to capture time and location data, and applies biometrics to ensure the accuracy and integrity of that data. A system administrator first registers the mobile device being used to record time and location data. At that time, a biometric registration is also performed. A mobile app can be prompted by a schedule or by the server to initiate a check-in, which in turn prompts a biometric capture. The time, location, and biometric capture are sent to the server, where it is matched and logged. The data is made available by API.



WebEnroll™

Browser-based biometric enrollment and data management

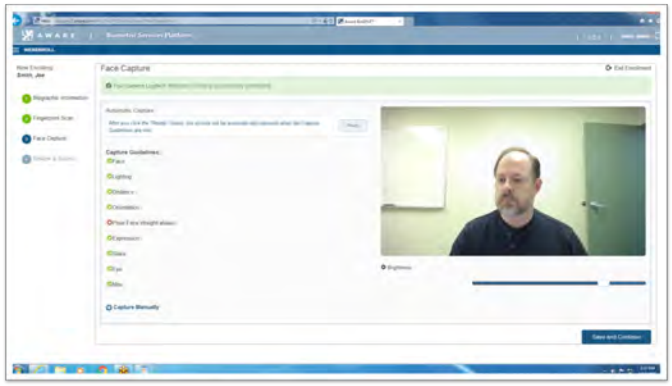
WebEnroll is a browser-based biometric enrollment and data management solution available as an enhanced version of BioSP™ (Biometric Services Platform) that utilizes BioComponents for capture of biographic data, fingerprints and facial images in a browser. Each BioComponent performs advanced biometric image autocapture as well as capture device hardware abstraction. Once images are captured, they are submitted to BioSP, where configurable workflows and modular software applications are used for processing, routing, and storage of each transaction. Biometric verification or identification can be added with Nexa or one of several third-party matchers integrated with BioSP, or an external matching service.



Biometric enrollment in a browser application - fingerprints

FEATURES AND FUNCTIONALITY

- **Upgrade to browser-based biometric enrollment using existing capture hardware peripherals**
- **No personally identifiable information (PII) stored on the workstation**
- **Most recent client software distributed and used automatically**



Biometric enrollment in a browser application - face

BioSP™ (Biometric Services Platform)

An open biometric workflow and middleware platform

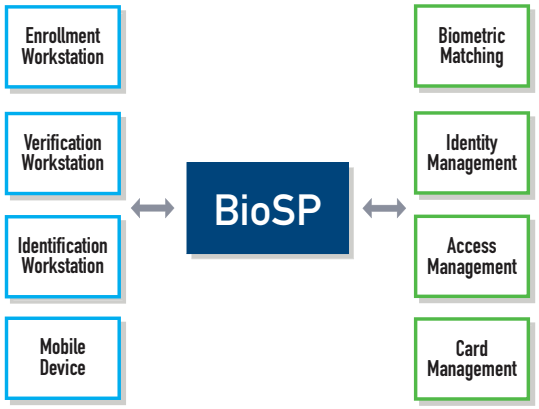
BioSP™ (Biometric Services Platform) is a modular, open platform used to enable a biometric system with advanced biometric data processing and management functionality in a web services architecture. It provides workflow, data management and formatting, and other important utilities for large-scale biometric systems.

BioSP is well suited for applications that require the collection of biometrics throughout a distributed network, and subsequent aggregation, analysis, processing, distribution, matching, and sharing of data with other system components. BioSP is modular, programmable, scalable, and secure, capable of managing all aspects of transaction workflow including messaging, submissions, responses, and logging. BioSP makes extensive use of open-source components and is Jakarta EE-compliant.

Security

BioSP is a secure system, with three mechanisms applied to securing data, communications, and access:

- User data access is provided by BioSP Logical Access module. This allows for both UI-level security and specific data security based an individual user groups and roles within the system.
- BioSP utilizes Hibernate technology to abstract the database communication; therefore, it can take full advantage of both Microsoft and Oracle database security and encryption of data at rest. For example, Oracle provides Transparent Data Encryption (TDE) in their 11G product; this ties the data within the database to either a software-based private key or a specific piece of hardware (HSM). Thus, in the event the data is stolen, it is useless without this private key.
- All communication to and from the BioSP server supports both SSL encryption as well as WS-Security. These two technologies prevent both man-in-the-middle and malicious client attacks.



FEATURES & FUNCTIONALITY

- Performs automated biometric image and data analysis, processing, formatting, quality assurance, and reporting
- Utilizes web services in support of a scalable, secure, service-oriented architecture (SOA)
- Integrates biometric functions with other enterprise systems such as identity management, access management, card management, and AFIS/ABIS
- Performs 1:1 and 1:many biometric matching for verification, identification, and duplicate checking
- Enables centralized system administration and user management
- Enables advanced reporting capabilities for fast troubleshooting of biometric capture problems
- Enables centralized configuration, distribution, and management of enrollment client software
- Supports fingerprint, face, iris, and palm modalities

Scalability

BioSP is a scalable and flexible system. Depending on the environment wherein it operates, there are five different areas were the system can scale:

- **BioSP employs load balancing functionality available through a Jakarta EE container application such as Apache Tomcat or Oracle WebLogic. This allows for both increased performance, since the processing is spread over multiple machines, and increased application uptime; if one server fails, another server would automatically take the additional traffic.**
- **BioSP runs in a Java Virtual Machine (JVM), so it can take advantage of multi-core processing.**
- **BioSP utilizes an open source workflow engine from Apache called ODE based on BPEL, which can be run in a separate application server from the business process logic. This allows for increased performance and throughput.**
- **BioSP has the ability to execute certain highly specialized biometric processing algorithms outside of the JVM, such as fingerprint matching algorithms. This allows these algorithms to be tuned to the specific operating system and processor on which they are executed, for maximum performance. Also, these algorithms communicate to the JVM through queuing mechanisms, which allows multiple algorithms to execute on separate machines in parallel.**
- **BioSP uses Hibernate technology to abstract the database from the JVM; therefore, it can run on multiple database platforms such as Oracle and Microsoft SQL Server. This allows full use of Microsoft and Oracle database scalability features such as replication, mass storage, and disaster recovery.**

Auditing

Audit trails are implemented with BioSP Logical Access and Event Manager. Logical Access provides support for security services in BioSP. It provides authentication and role-based authorization features. Logical Access deals with the following entities: Users, Roles, and Resources. A user can have multiple roles. A role can access a set of resources that are secured. These secured resources can be data within BioSP, user interface components of BioSP, or any custom defined resources.

APPLICATIONS

- **ABIS/AFIS integration**
- **Citizen ID and voting programs**
- **Know Your Customer**
- **Fraud prevention**
- **Border management**
- **Mobile biometric authentication**
- **Law enforcement**
- **Defense**

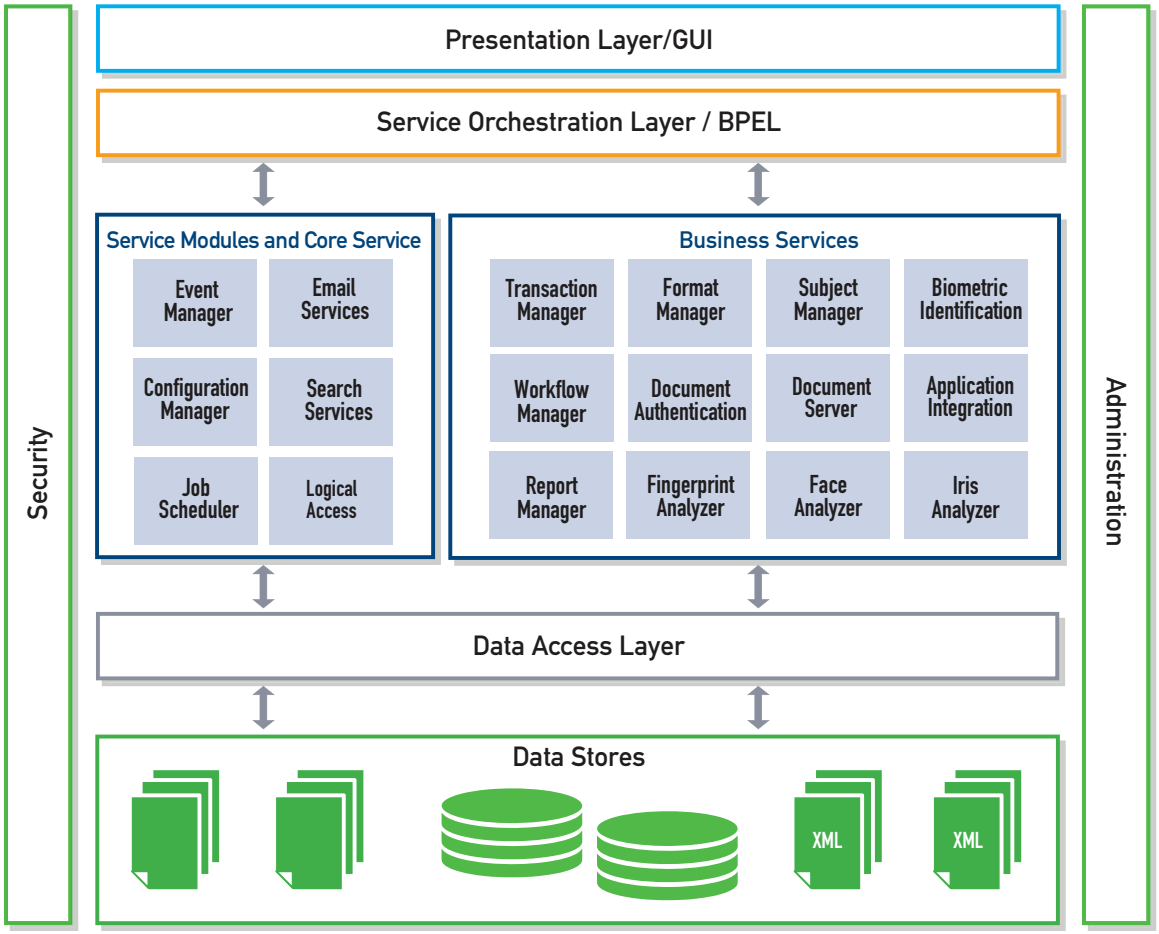
Log Manager provides services to record and monitor business events in BioSP. The logs can be categorized based on types and monitored separately. The basic functions performed by LogManager are: 1) add a log 2) find logs based on criteria 3) associate a new log with a previously existing parent log.

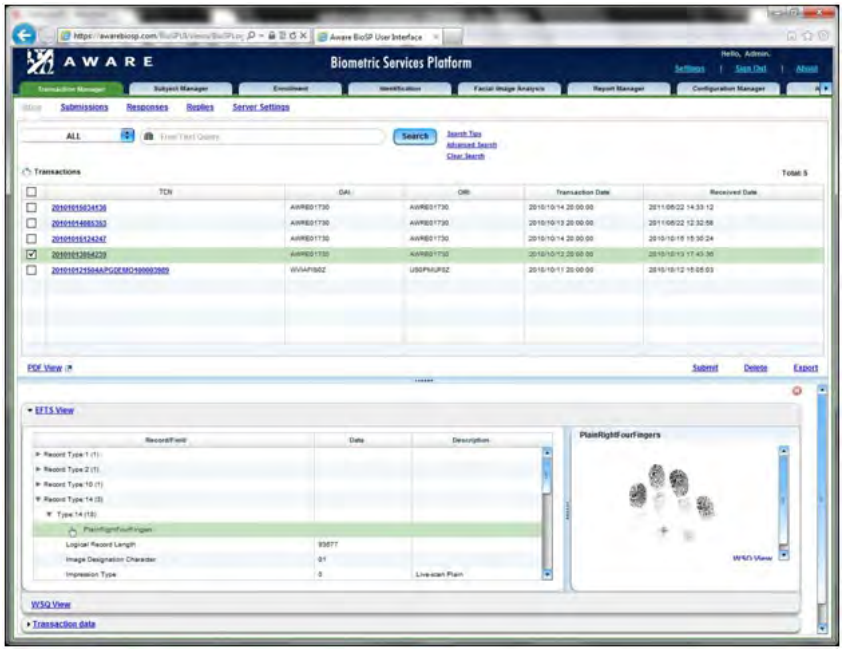
Role-Based User and Group Resource Access and Passwords

BioSP offers improved resource access control. Features in the UI and services provided by the BioSP server can be viewed as resources. Access to these resources by users can be configured.

BioSP supports the concept of roles. A user with a given role is given permission to access a resource in a specific manner. For example, a user may be assigned to a role that allows them to see a list of transactions but not to see the individual NIST fields in the transactions. Another user may have permission to see the transactions and their contents but not to edit them.

BioSP supports the concept of groups. A group is a logical grouping of users. This allows BioSP to support functionality such as dividing users into groups. Groups are independent of roles; a user can have multiple roles and belong to multiple groups.





BioSP browser-based user interface

BioSP Modules

BioSP offers many advanced biometric capabilities, available through independent, service-oriented software modules. Each BioSP module performs a discrete set of functions, including biometric authentication, search, and duplicate checking, centralized image and data analysis and processing, data formatting and transcoding, and image quality assurance and reporting. The modules interact with each other via web services.

CORE

BioSP Core provides the central infrastructure services shared across BioSP modules and business processes. Core is required to run other BioSP modules, which may be added and modified incrementally as business needs evolve. Components of the Core include the Web Services engine, security, Business Process Execution Language (BPEL) engine, email support, job scheduler, user management, logical access control, search services, document storage, and logging.

BioSP uses BPEL to allow for quick scripting of biometric-centric use cases. BPEL is an open, standardized scripting language that orchestrates services, operations, and criteria to automate business processes defined in XML. Lower-level operations defined in BioSP modules are aggregated in BPEL scripts to form composite services. These composites enable synchronous and asynchronous processing of transactions and data to meet the requirements of a wide variety of use case scenarios.

WORKFLOW MANAGER

BioSP Workflow Manager allows stateful processing workflow that involves user interaction, such as approvals, reviews, or edits. The workflow is scripted using BPEL, which allows it to be easily modified to many use cases. Each state of the workflow can have a different owner, and history is tracked over the lifecycle. Workflow Manager also allows for manual adjudication of tasks. The operator is presented with task input data, they are prompted for a decision, and the task output data is saved and used to finish the overall workflow.

TRANSACTION MANAGER

BioSP Transaction Manager provides services for building transaction workflows between multiple disparate systems, including enrollment clients and other back-end systems. It is driven by BPEL workflow definitions and is highly configurable, managing both receipt of submissions and processing of responses from distributed sources. Store-and-forward requirements for standards-based communication with local, state, federal, and international government agencies are addressed with Transaction Manager.

SUBJECT MANAGER

BioSP Subject Manager provides services for managing and archiving subject identity data, both biographic and biometric, as well as custom metadata. Subject Manager manages the server side of biometric enrollment processes, the collection of biometric samples (images or templates) and biographic data for credentialing, biometric identification, or biometric verification. It provides support for finger, face, palm, iris, and scar/mark/tattoo images.

FORMAT MANAGER

BioSP Format Manager provides services for working with various open standards data formats to enable interchange of biometric and biographic data. Format Manager parses, validates, constructs or transcodes standard-compliant biometric data structures, including those formats defined by ANSI/NIST, ANSI/INCITS, ISO/IEC, FIPS-201, and ICAO.

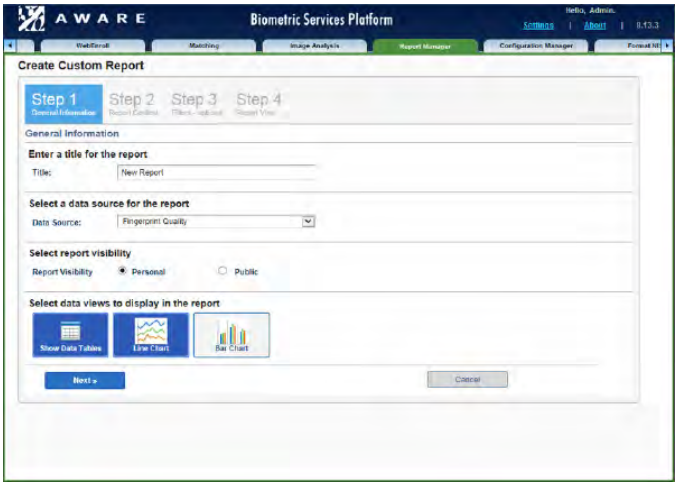
BIOMETRIC IDENTIFICATION

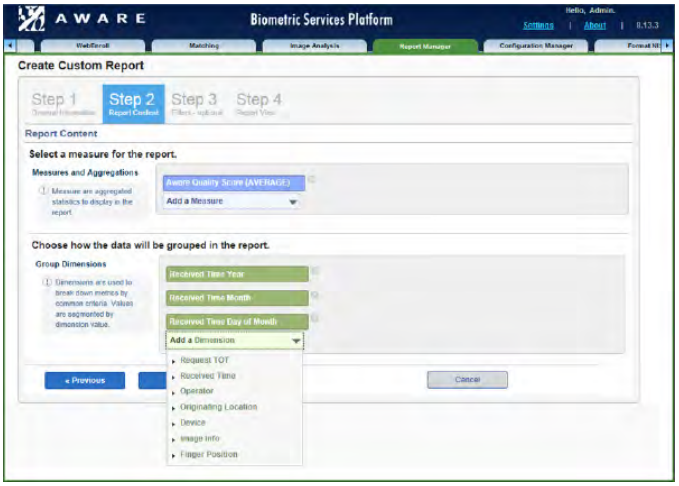
BioSP Biometric Identification module provides several biometric matching services, including one-to-one and one-to-many matching for authentication/verification, identification, and duplicate checking. Matching algorithms from Aware or third-parties may be integrated or called using BioSP BPEL services. Multiple matchers can be integrated. With its abstracted Web-services based API, it enables users to use a single implementation and set of instructions with multiple matchers.

REPORT MANAGER

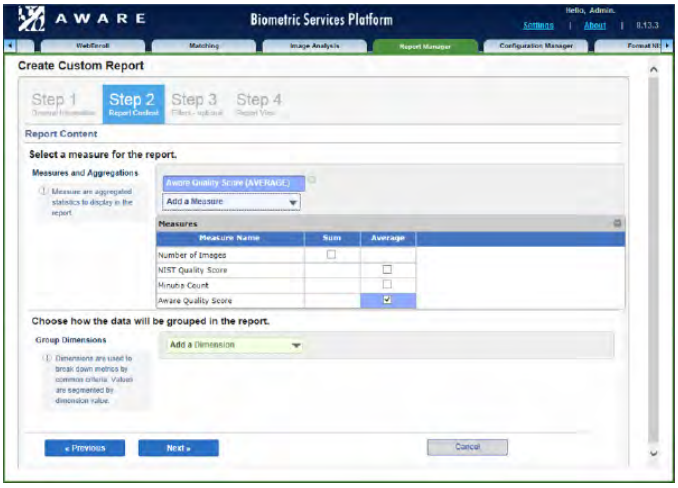
BioSP Report Manager and associated modules provide biometric data collection, statistical analysis, and customizable reporting by processing and presenting data generated by Format Manager and the Fingerprint Analysis, Facial Analysis, and Iris Analysis modules. Biometric transactions are analyzed for image quality problems and non-conformance errors, and the resulting data is made available for users to retrieve, organize, and visualize in the form of custom, graphical reports. The reports can be used to identify and troubleshoot enrollment problems, quantify environmental factors, and perform general system performance monitoring and improvements.

Creating a New Report

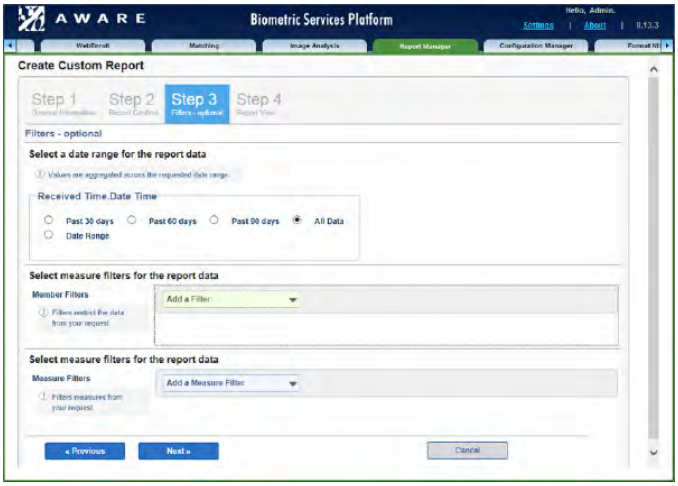




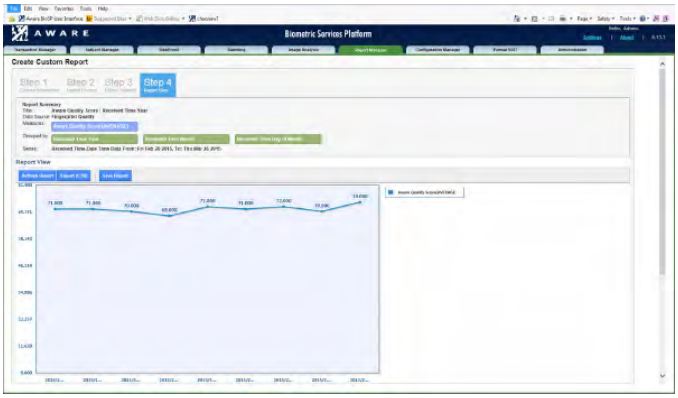
Designing a New Report



Modifying a Report with Filters



Displaying a Report



FINGERPRINT ANALYZER

BioSP Fingerprint Analyzer module provides services for complex fingerprint processing tasks and workflows. Quality assessment, segmentation, compression, decompression, and other processing tools are provided by this module.

FACE ANALYZER

BioSP Face Analyzer module is designed for remote, web-based submission of facial images for compliance analysis against standards-based or custom profiles. Profiles contain values that must be attained in order for a facial image to be considered in compliance with a standard (e.g. ISO/IEC 19794-5 for e-passports).

Users submit electronic facial images individually or in batches via an easy-to-use web interface or web service call. They are presented with results in real time, including pass or fail, and descriptions of problems in the case of a failure. Compliant images generated by the module may be stored in BioSP for integration with other systems (e.g. CMS), returned to the user, or both.

See PreFace for more details about Face Analyzer capabilities.

IRIS ANALYZER

BioSP Iris Analyzer performs centralized iris image segmentation and quality scoring using IrisCheck libraries. Quality vectors and scores are defined according to the international biometric iris image quality standard ISO/IEC 29794-6. See IrisCheck for more details about Iris Analyzer capabilities.

CONFIGURATION MANAGER

BioSP Configuration Manager performs centralized management of client enrollment application configuration, enabling a high degree of automation of client software distribution and maintenance. Software updates are automatically downloaded from BioSP to remote clients, and take into account local client configuration and conditions, such as capture hardware model and version. Access to software updates is securely controlled.

DOCUMENT SERVER

BioSP Document Server performs customizable PDF document generation from submitted biometric images and data transactions. It performs layout of biometric images, biographic data, and other data such as barcodes into documents according to configurable layout design files. Biometric data transactions are submitted to Document Server, which returns a PDF representation of the images and data according to the prescribed layout file. Document Server incorporates Aware's AccuPrint™, an FBI-certified software product for creation of printed documents containing fingerprint images.

Astra™

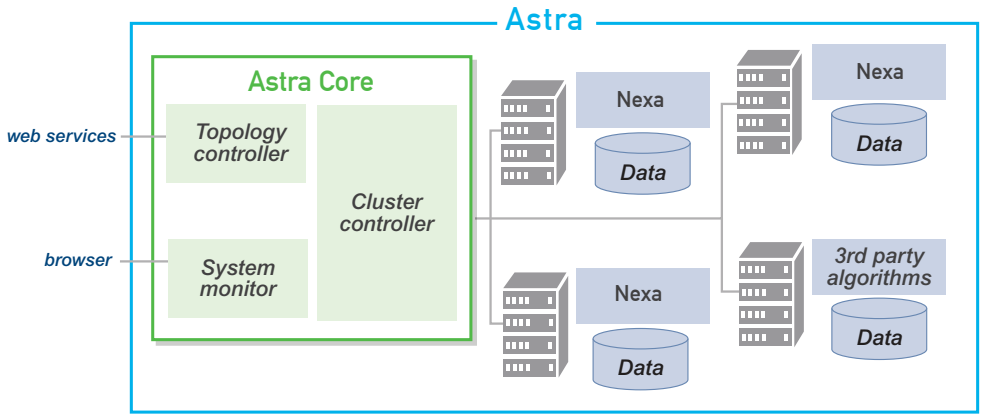
An algorithm-independent cluster computing platform for highly scalable biometric matching

Astra™ is a cluster computing platform used for large-scale biometric identification and deduplication using fingerprint, face, and iris recognition. It is a highly scalable platform that performs one-to-many search or one-to-one match against large stores of biometrics and other identity data. It does so by deploying biometric data and matching algorithms across a cluster of multiple computing nodes.

Extremely large biometric databases (tens of millions of records) cannot be stored or efficiently searched on a single computer. Distributing the data and biometric comparison tasks across multiple machines enables even extremely large databases to be searched in only seconds. Astra enables not only massive biometric search tasks but complex filter, search, match, and link operations critical to data preparation and quality assurance functions such as identity resolution and data deduplication.

APPLICATIONS

- Automated fingerprint identification system (AFIS)
- Large-scale biometric identification and deduplication
- High-volume, high-availability biometric authentication
- Large-scale identity data quality analysis, identity resolution, and link analysis
- Citizen ID



FUNCTIONALITY

- Fingerprint recognition
- Facial recognition
- Iris recognition
- Distributed biometric and text search and match across multiple computing nodes
- Support for fingerprint, face, iris, voice, and other biometric modalities
- Support for text-based pre-filtering of biometric search
- Support for text-based identity search, match, and link algorithms
- Identity data deduplication
- Data quality analysis
- Identity resolution
- Link analysis and relationship discovery

Astra makes use of an open source distributed computing framework that is in use in a diverse variety of large-scale systems, and thus is field-proven, reliable, and well-supported. Astra is highly fault-tolerant with integrated failover capability, and includes a browser-based system monitoring dashboard that allows administrators to know the performance of the system at all times and be alerted when problems arise.

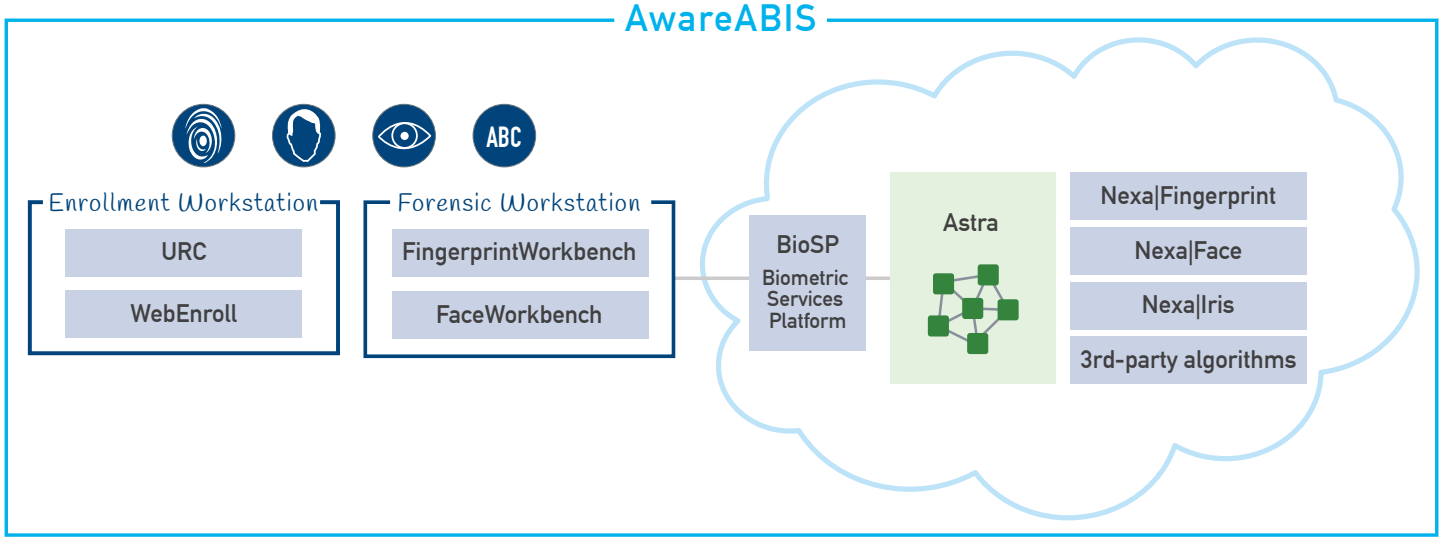
Astra configures a multi-node computing topology and deploys the algorithms and data for fingerprint, face, and iris recognition to each node, then manages the execution of the millions of operations and results in such a way that maximizes the utilization of the machines and processors. The platform is independent of the algorithms in use, so long as access to 1:1 matching capability of the algorithm is provided. The platform is able to run one or more biometric and text matching algorithms in either staged or parallel search configurations.

FEATURES

- **Highly scalable**
- **Fault-tolerant**
- **Algorithm-independent**
- **Open source-based components**
- **Support for multi-stage algorithms**
- **In-memory template storage**
- **Browser-based system monitoring and reporting**

Astra Core provides system configuration, management, and monitoring. System topology and workflows are configured. The biometric data cache is managed. Biometric matching algorithms are configured, managed and deployed. A browser-based system monitoring dashboard provides alerts and statistical information about the operation of the system. The cluster controller executes commands and computations across multiple computing nodes. It deploys biometric and text matching algorithms and data to each node.

Astra used in AwareABIS



Nexa™ |Fingerprint

SDK for fingerprint-based biometric identification and authentication

Nexa|Fingerprint provides high-performance biometric algorithms for multistage fingerprint recognition and identification or rapid, high-volume fingerprint authentication. Nexa APIs are reliable, configurable, and easy to use, complemented by a level of technical support that has helped make Aware a trusted provider of high-quality biometric software for over twenty years.

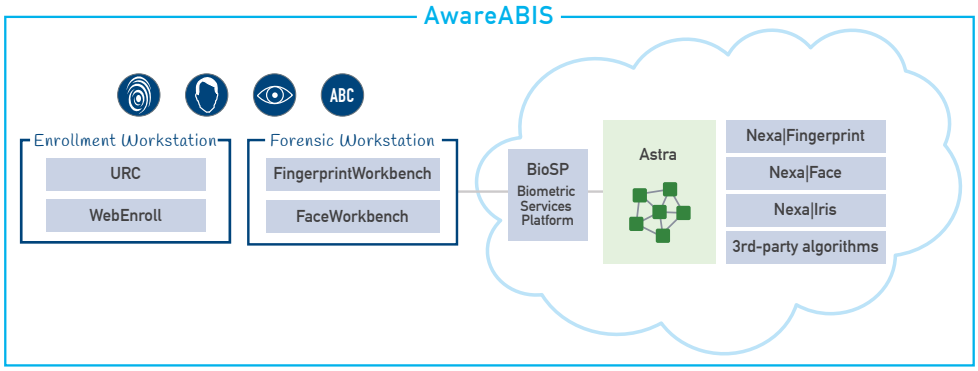
Nexa SDKs are designed to be easily configured towards optimization of a system for a given application, database, computing platform, and operational environment. They include tools that help quantify system performance, identify opportunities for improvement, and continuously optimize the system.

Fast, Accurate, and Scalable

- **Well-designed, easy-to-use APIs**
- **Support for authentication, identification, and deduplication**
- **Human-interpretable match and confidence scores**
- **Fully scalable and extensible**
- **Tunable for performance optimization**
- **Seamless operation with Aware's other modular products**

Nexa|Fingerprint used in AwareABIS™

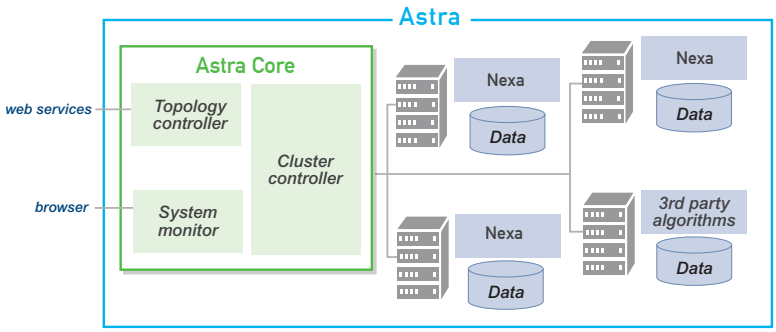
AwareABIS™ is an Automated Biometric Identification System (ABIS) used for large-scale biometric identification and deduplication, with support for fingerprint, face, and iris modalities. Its highly modular architecture allows it to be configured and optimized for either civil or criminal applications.



It has the flexibility to utilize Aware's high-performance, NIST-tested Nexa™ face, fingerprint, and iris matching algorithms, as well as top-tier fingerprint algorithms from 3rd-party providers. Together, these features make it the best ABIS on the market not only for extreme

Nexa|Fingerprint used in Astra™

Astra™ is a cluster computing platform used for large-scale biometric identification and deduplication using fingerprint, face, and iris recognition. It is a highly scalable platform that performs one-to-many search or one-to-one match against large stores of biometrics and other identity data. It does so by deploying biometric data and matching algorithms across a cluster of multiple computing nodes.



Nexa™ |Face

SDK for facial recognition and authentication

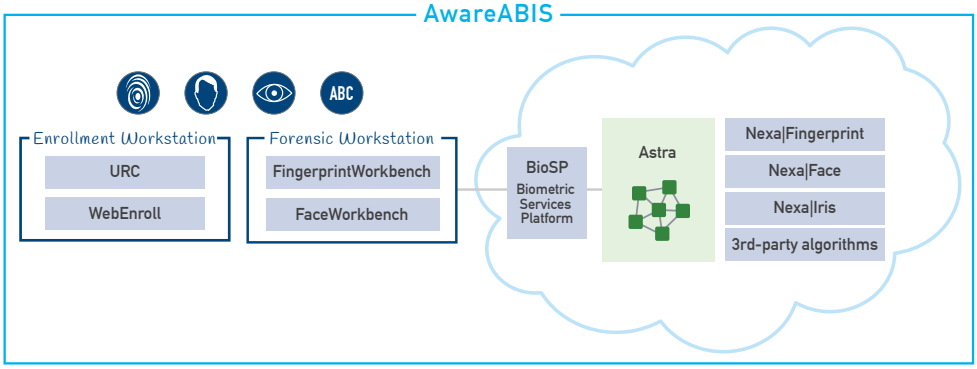
Nexa|Face™ provides high-performance biometric algorithms for multistage facial recognition and identification or rapid, high-volume face authentication. Nexa APIs are reliable, configurable, and easy to use, complemented by a level of technical support that has helped make Aware a trusted provider of high-quality biometric software for over twenty years.Nexa SDKs are designed to be easily configured towards optimization of a system for a given application, database, computing platform, and operational environment. They include tools that help quantify system performance, identify opportunities for improvement, and continuously optimize the system.

Fast, Accurate, and Scalable

- Well-designed, easy-to-use APIs
- Support for authentication, identification, & deduplication
- Human-interpretable match and confidence scores
- Fully scalable and extensible
- Tunable for performance optimization
- Seamless operation with Aware's other modular products

Nexa|Face used in AwareABIS™

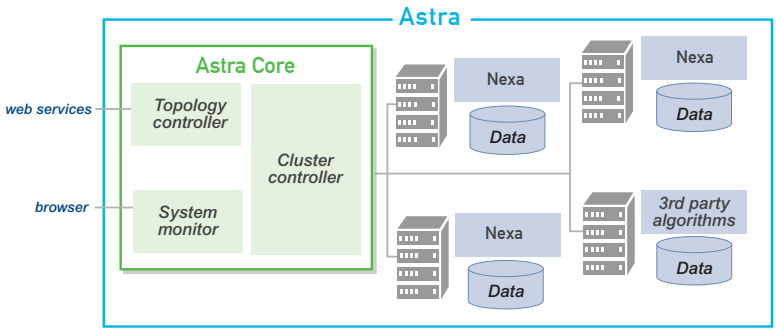
AwareABIS™ is an Automated Biometric Identification System (ABIS) used for large-scale biometric identification and deduplication, with support for fingerprint, face, and iris modalities. Its highly modular architecture allows it to be configured and optimized for either civil or criminal applications.



It has the flexibility to utilize Aware's high-performance, NIST-tested Nexa™ face, fingerprint, and iris matching algorithms, as well as top-tier fingerprint algorithms from 3rd-party providers. Together, these features make it the best ABIS on the market not only for extreme configurability but for prevention of vendor lock-in.

Nexa|Face used in Astra™

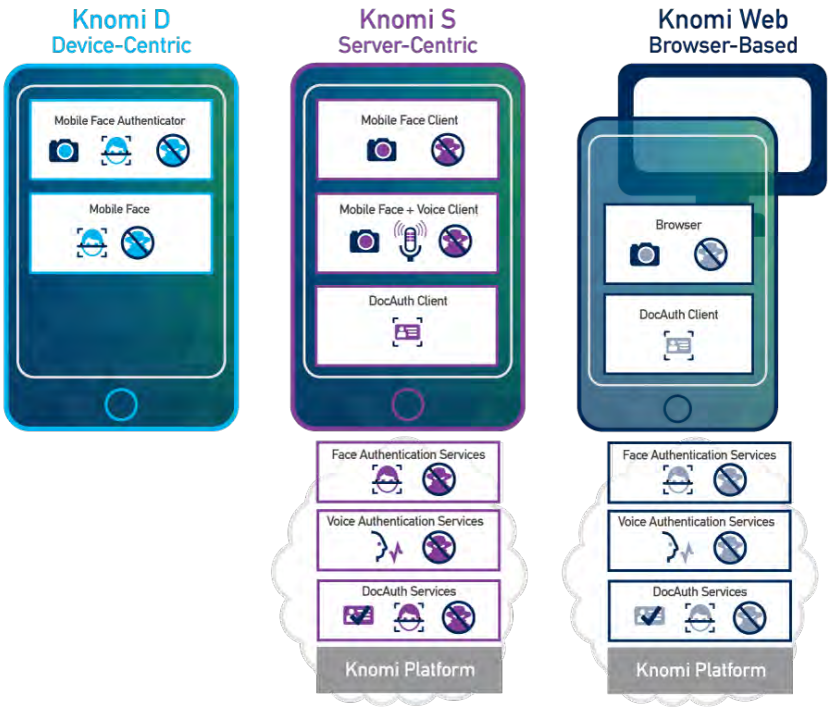
Astra™ is a cluster computing platform used for large-scale biometric identification and deduplication using fingerprint, face, and iris recognition. It is a highly scalable platform that performs one-to-many search or one-to-one match against large stores of biometrics and other identity data. It does so by deploying biometric data and matching algorithms across a cluster of multiple computing nodes.



Nexa|Face used in Knomi®

Knomi® is a mobile biometric authentication solution comprised of a family of biometric matching and liveness detection algorithms that use face and voice to enable secure and convenient multifactor authentication without passwords.

Knomi can also be used for identity proofing as part of a mobile onboarding solution, with advanced security checks that authenticate driver's licenses and passports, and spoof-resistant biometric facial matching between the live and printed images.



Nexa™|Iris

SDK for iris recognition and authentication

Nexa|Iris™ is a high-performance iris recognition and authentication algorithm. Nexa APIs are reliable, configurable, and easy to use, complemented by a level of technical support that has helped make Aware a trusted provider of high-quality biometric software for over twenty years.

Nexa SDKs are designed to be easily configured towards optimization of a system for a given application, database, computing platform, and operational environment. They include tools that help quantify system performance, identify opportunities for improvement, and continuously optimize the system.

Fast, Accurate, and Scalable

Well-designed, easy-to-use APIs

Fully scalable and extensible

Tunable for performance optimization

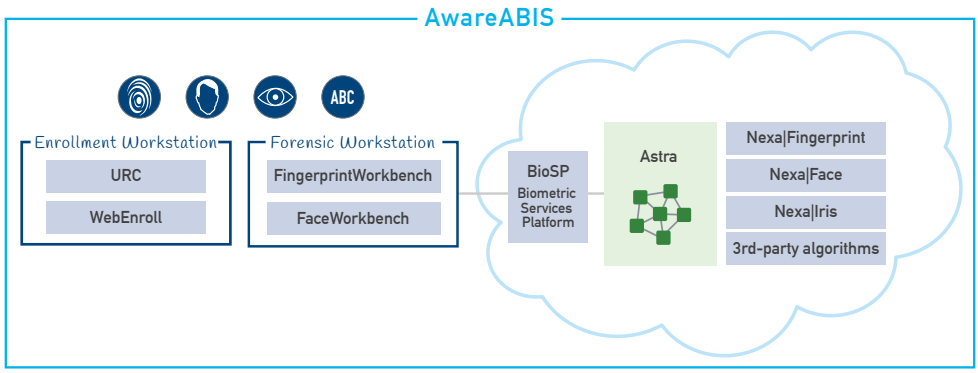
Support for authentication, identification, and deduplication

Human-interpretable match and confidence scores

Seamless operation with Aware's other modular products

Nexa|Iris used in AwareABIS™

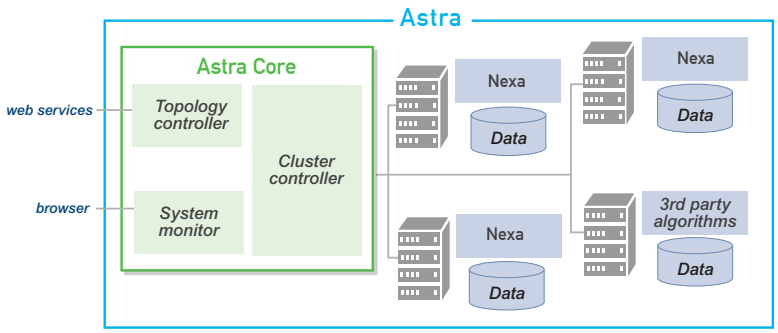
AwareABIS™ is an Automated Biometric Identification System (ABIS) used for large-scale biometric identification and deduplication, with support for fingerprint, face, and iris modalities. Its highly modular architecture allows it to be configured and optimized for either civil or criminal applications.



It has the flexibility to utilize Aware's high-performance, NIST-tested Nexa™ face, fingerprint, and iris matching algorithms, as well as top-tier fingerprint algorithms from 3rd-party providers. Together, these features make it the best ABIS on the market not only for extreme configurability but for prevention of vendor lock-in.

Nexa|Iris used in Astra™

Astra™ is a cluster computing platform used for large-scale biometric identification and deduplication using fingerprint, face, and iris recognition. It is a highly scalable platform that performs one-to-many search or one-to-one match against large stores of biometrics and other identity data. It does so by deploying biometric data and matching algorithms across a cluster of multiple computing nodes.



Nexa™ |Voice

Mobile voice authentication SDK

Nexa|Voice is an SDK that offers biometric speaker recognition algorithms, software libraries, user interfaces, reference programs, and documentation to use voice biometrics to enable multi-factor authentication on iOS and Android devices. Biometric template storage and matching can be performed either on a mobile device or on a server. Nexa|Voice APIs are reliable, configurable, and easy to use, complemented by a level of technical support that has helped make Aware a trusted provider of quality biometric software and solutions for over twenty-five years.

High-performance biometric speaker recognition for convenient and secure multifactor authentication

Top-tier algorithm performance

Language-independent

Fusion with other modalities

Static or dynamic passphrase options

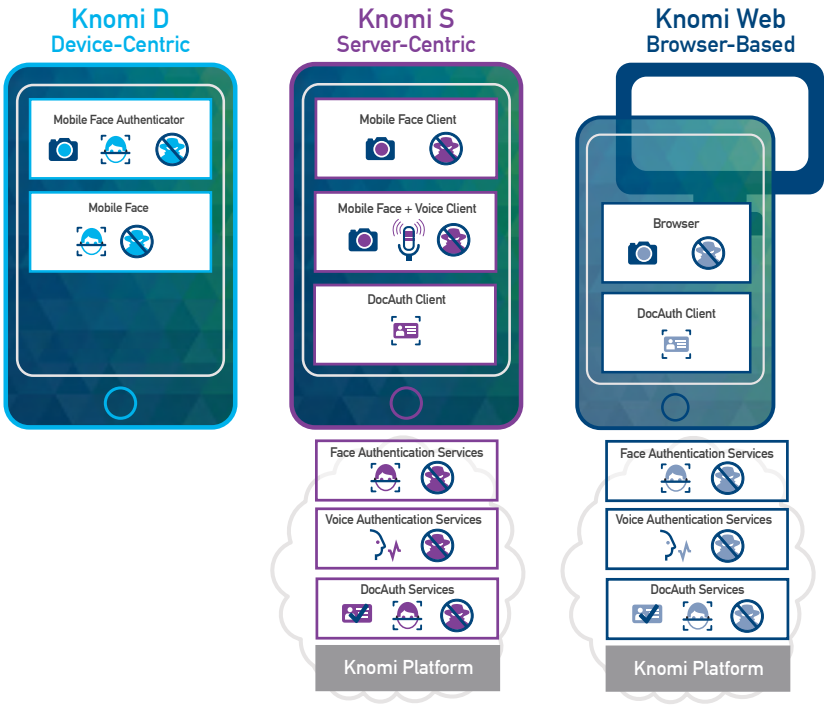
Liveness detection

Collaborative technical support

Nexa|Voice used in Knomi®

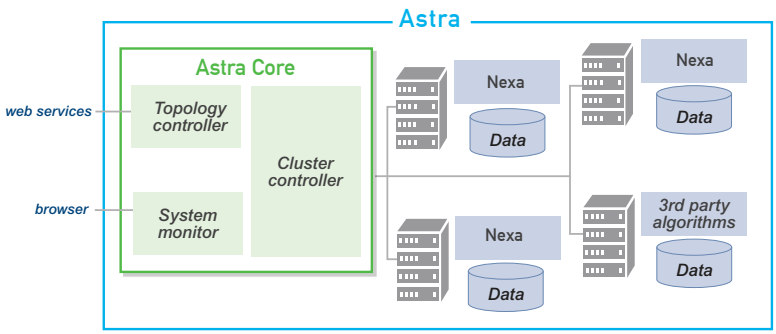
Knomi® is a mobile biometric authentication solution comprised of a family of biometric matching and liveness detection algorithms that use face and voice to enable secure and convenient multifactor authentication without passwords.

Knomi can also be used for identity proofing as part of a mobile onboarding solution, with advanced security checks that authenticate driver's licenses and passports, and spoof-resistant biometric facial matching between the live and printed images.



Nexa|Voice used in Astra™

Astra™ is a cluster computing platform used for large-scale biometric identification and deduplication using fingerprint, face, and iris recognition. It is a highly scalable platform that performs one-to-many search or one-to-one match against large stores of biometrics and other identity data. It does so by deploying biometric data and matching algorithms across a cluster of multiple computing nodes.



AwareXM™

MINEX-certified, ANSI/INCITS 378-compliant fingerprint minutiae extraction, template generation, and matching for biometric verification

AwareXM is an SDK that provides MINEX-certified, INCITS 378-compliant fingerprint minutiae extraction, template generation, and biometric verification, such as required for PIV credential personalization and authentication. AwareXM includes other features, such as Aware's QualityCheck™ and NFIQ fingerprint image quality scoring. AwareXM provides support for several biometric standards including ISO/IEC 19794-2 for minutiae-based template data formatting and ILO SID-0002 for seafarer identity cards.

Because AwareXM is MINEX-certified, it is interoperable with template extraction and matching algorithms from many other vendors. This means that fingerprint templates generated and stored on a card using AwareXM can be biometrically verified by any other MINEX-certified matcher. Conversely, AwareXM can be used to verify any template generated by a MINEX-certified extraction algorithm.

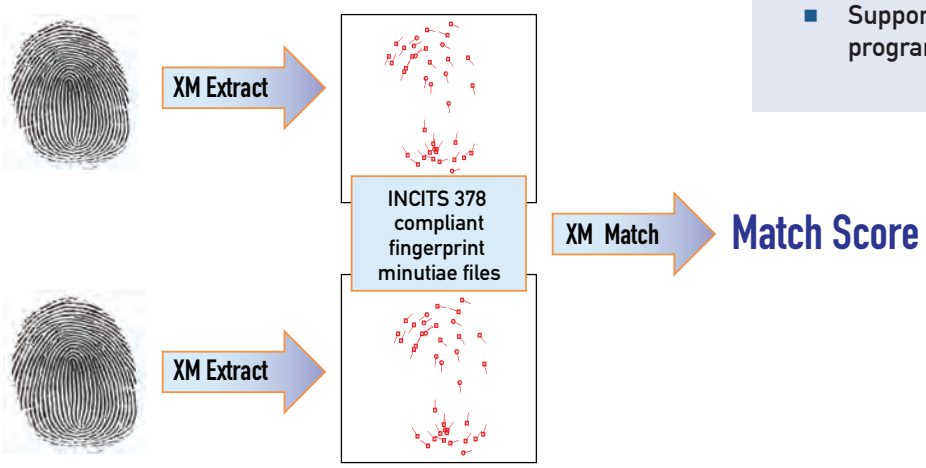
AwareXM works seamlessly with PIVPack and ICAOPack to incorporate biometric verification into a comprehensive enrollment, personalization, and reader software solution.

APPLICATIONS

- Fingerprint verification
- Authentication
- Access control
- Citizen ID
- Access control
- Credentialing

FEATURES AND FUNCTIONALITY

- MINEX-certified, interoperable fingerprint template extraction and matching
- Optional performance-optimized (non-interoperable) template extraction matching
- INCITS 378 compliant template generation
- Support for ISO/IEC 19794-2:2011 data formatting and parsing
- Support for ILO SID-0002 seafarer ID cards
- Support for a variety of image input formats
- Fingerprint quality scoring, including NFIQ
- Support for C, C# .NET, and Java programming languages



About MINEX and PIV

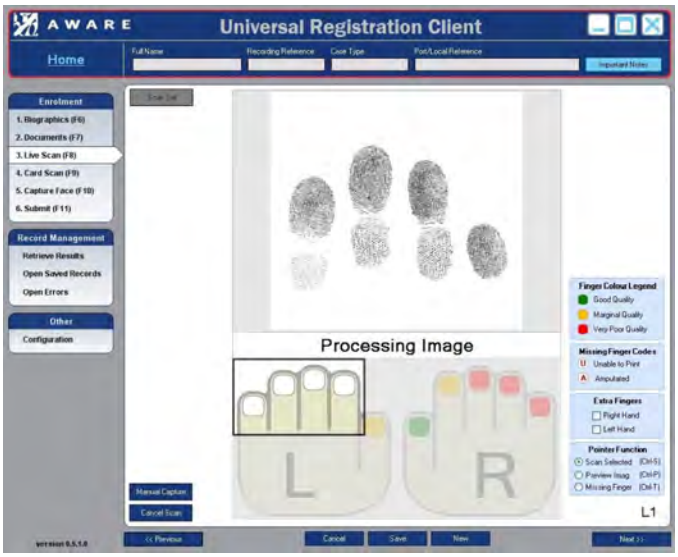
NIST is the National Institute of Standards and Technology, a U.S. government agency. In order to assess the interoperability of fingerprint minutiae templates—that is, could minutiae extracted by one algorithm be matched by an algorithm of other vendors—they conducted a test called MINEX. The test was conducted primarily to assess whether fingerprint minutiae-based templates could achieve a sufficient level of interoperability for effective biometric verification (low false accept and false reject rates), or rather would images be required. A requirement for participation in the MINEX test is ANSI/INCITS 378 compliance. ANSI/INCITS 378 is a standard for fingerprint template data formatting. On an on-going basis, the MINEX tests yield lists of both extract algorithms and match algorithms that achieved a minimum threshold of performance when used in conjunction with algorithms of the various participants, and are thus “MINEX-certified”.

The FIPS 201 standard for “PIV” federal employee credentialing requires that fingerprint templates from two fingers be stored on each ID card in INCITS 378 format. GSA requires that only extraction algorithms certified by the MINEX test be used to generate templates for storage on PIV ID cards.

Universal Registration Client (URC™)

Software application for biometric enrollment

Universal Registration Client (URC) is a configurable Windows-based .NET application that utilizes BioComponents™ and Aware SDKs to perform a variety of biometric data capture, analysis, matching, formatting, and hardware abstraction functions. All BioComponents can operate within URC. Source code is available for URC, so it can be used either to quickly learn how to best implement BioComponents and SDK APIs, or alternatively as a baseline to develop an application customized for custom requirements and workflow.



APPLICATIONS

- Fingerprint recognition, face recognition, iris recognition
- Automated fingerprint identification services (AFIS)
- Automated biometric identification services (ABIS)
- Border management
- Citizen ID
- Defense and intelligence
- Law enforcement

FEATURES AND FUNCTIONALITY

- Biographic data capture, formatting, and validation
  - ANSI/NIST-ITL 2013 and earlier
  - ICAO Doc 9303
  - FIPS 201 SP
  - 800-76
- Tenprint autocapture
- Fingerprint matchability testing
- Fingerprint segmentation and sequence checking
- Fingerprint quality scoring
  - Aware Quality
  - NFIQ
- Fingerprint card scanning and printing
- Fingerprint template extraction and 1:1 matching for biometric authentication
- Facial image autocapture
- Iris capture and quality scoring
- Handwritten signature capture
- Travel document scanning and authentication
- Credential personalization
  - ICAO compliant e-passport
  - FIPS 201 compliant PIV card
- Digital certificate verification
- Biometric duplicate checking
- Web service-based connectivity to BioSP

URC|Mobile™

Biometric enrollment application optimized for android tablets

URC|Mobile™ is a software application for capturing fingerprint and facial images on an Android tablet using its onboard camera and an integrated fingerprint capture device. It is designed to be used by an enrollment attendant for rapid capture and quality assurance of biometric data and submission to a centralized biometric database for enrollment, search, or authentication. URC|Mobile is best suited for an environment where mobility beyond a desktop is useful, or where a more economical client platform than can be supported with a desktop solution.

URC|Mobile consists of a user interface for capture of biographics, fingerprint, and face, and utilizes Aware software libraries found in the mobile version of the following SDKs:

PREFACE MOBILE **– facial image autocapture, quality assurance, and optimization**

LIVESCAN API MOBILE **– fingerprint image capture and device abstraction**

NISTPACK MOBILE **– file structuring and validation**

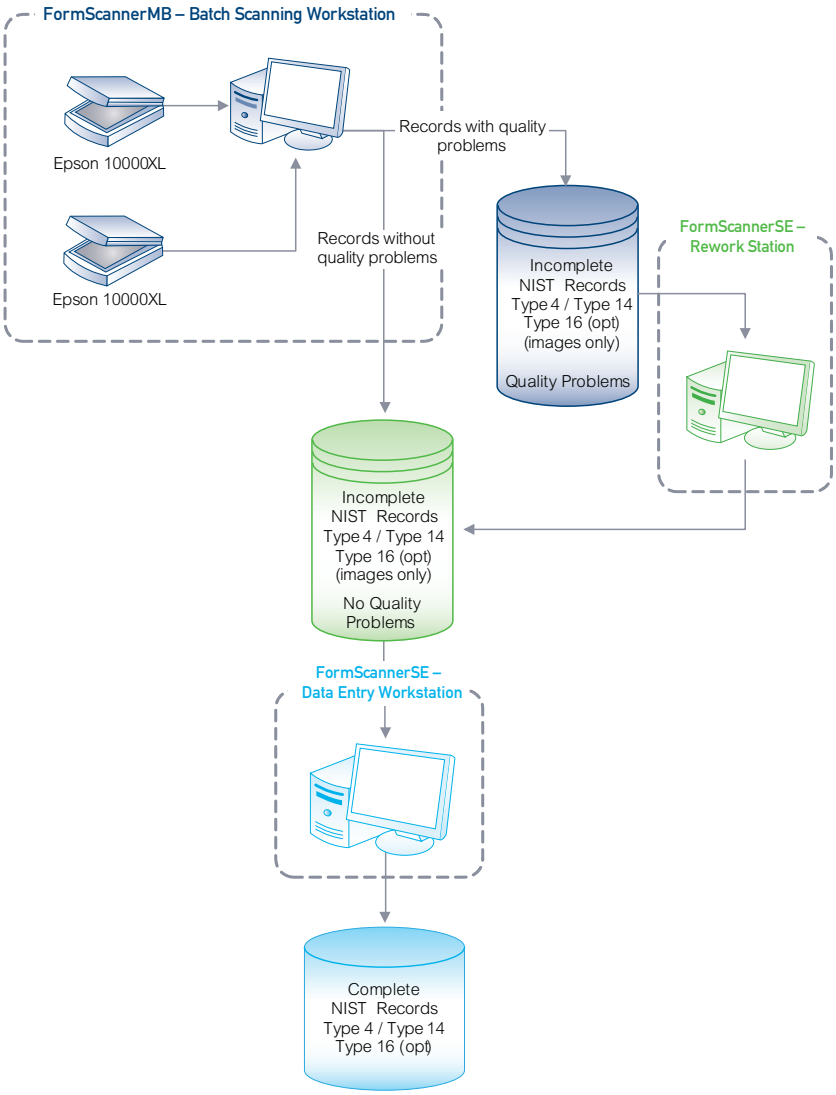
WSQ1000 MOBILE **– fingerprint image compression**

FormScanner™

FBI-certified software applications for single and multi-batch scanning of fingerprint cards and conversion to NIST records

FormScannerSE™ and FormScannerMB™ are two independent applications for scanning and processing of inked fingerprint cards. They are available separately or as a bundle. FormScannerSE is designed for one-at-a-time, assisted "scan and entry" processing of fingerprint cards, such as for manual data entry of previously scanned card batches. It can also be used for manual "rework" such as crop region adjustments. FormScannerMB is designed for "multi-batch" scanning of large volumes of cards in an automated fashion, and provides features useful for high-volume processing such as support for automatic document feeding and real-time image quality feedback.

Both FormScanner applications use a template-driven workflow to support the processing of any card or form type. They automatically identify the finger images present on the form, crop them, and perform quality analysis, segmentation, sequence checking, compression, and data structuring as ANSI/NIST-ITL Type-4 or Type-14, and (optional) Type-20 records. They each utilize Aware's AccuScan, NISTPack, and SequenceCheck SDKs. AccuScan is certified by the FBI and compliant with FBI image quality specifications (IQS).



APPLICATIONS

- **Fingerprint recognition,**
- **Automated fingerprint identification services (AFIS)**
- **Border management**
- **Citizen ID and voting systems**
- **Defense and intelligence**
- **Law enforcement**

Functionality Summary

Common Features	■ FBI-certified card scanning solution ■ Lossless JPEG 2000 compression of full card images (for Type-20 records) ■ WSQ compression (for Type-4/14 records) ■ Sequence checking ■ Fingerprint image quality scoring ■ Parsing, creation, and validation of ANSI/NIST-ITL 2013 (and earlier) Type-4, Type-14, and Type-20 records ■ Template-based cropping of images with a template creation program ■ OCR-assisted card alignment ■ Barcode reading ■ Interface to external systems for record input/output ■ Web service connectivity to BioSP
FormScannerSE "Scan and Entry"	For manual, single card "scan and entry": ■ Manual, assisted data entry ■ NIST record creation For file rework: ■ NIST record parsing ■ Crop region adjustments ■ Sequence error correction ■ NIST record output ■ Card orientation check
FormScannerMB "Multi-Batch"	For automated conversion of high volumes of fingerprint cards and forms to digital NIST records: ■ Support for two-sided forms ■ Support for automatic document feeders (ADF) ■ Support for use of multiple scanners simultaneously ■ Paper jam resolution ■ Automated, configurable quality analysis and categorization ■ Real-time, graphical quality reporting ■ Mid-batch low-quality alerts ■ Post-batch card quality summary report ■ Batch status dashboard (# batches, # transactions, etc.)

FormScannerSE™

FormScannerSE is a software application designed to assist the process of scanning and processing of fingerprint cards and forms. Used with off-the-shelf consumer-grade flatbed scanners, it utilizes three Aware SDKs: AccuScan, NISTPack, and SequenceCheck, and is FBI certified.

The user interface implements workflow designed to enable the operator of the workstation to scan the form, make corrections, and manage the manual entry of the biographic data contained on the form. The section of the form containing the biographic data is displayed on the top half of the screen and the data entry boxes of the application are displayed on the bottom half of the screen. As the user moves the cursor to the selected data entry box, the scanned form pans and scrolls automatically in the top half of the screen so the original biographic data in typed or handwritten form is display prominently to assist keyed data entry.

A "rework station" equipped with FormScannerSE can be used to manually perform crop region adjustments, fix sequence errors, and perform data entry on forms previously scanned using FormScannerMB in a batch-scan process.

Automated, reworkable fingerprint image cropping

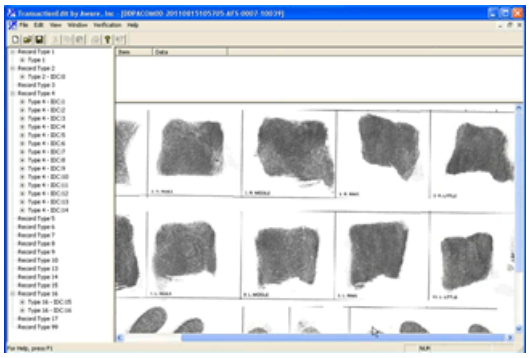
Manual entry of additional field values

FormScannerMB™

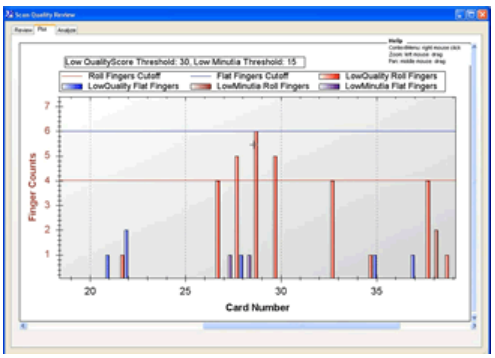
FormScannerMB is a software application designed for high-volume fingerprint card scanning and conversion to skeletal NIST records. It operates in batch mode with one or more certified scanners such as the Epson 10000XL. Use of automatic document feeders (ADF) are supported, and two-sided form scanning is supported through the duplexer option available with certain Epson scanner models. The application enables full management of the scanner, with functions for setting up batch jobs, starting and stopping jobs, and handling paper jams. Multiple scanners operating simultaneously are supported from a single workstation.

Reports on image quality can be generated during and following the scan of a batch. Configurable quality thresholds can be set, and automatic alerts are generated when thresholds are not met. This is to alert an operator to problems before large quantities of forms are scanned improperly.

FormScannerMB outputs "skeletal" NIST records to which biographics and metadata from the cards can be added later (using FormScannerSE). Either Type-4 or Type-14 records containing WSQ images can be included in the output transaction. Type-20 records containing a lossless JPEG 2000 compressed image of the front and back of each card can optionally be included.



File viewer



Batch quality reporting

FormScannerSWFT™

FormScannerSWFT is a version of FormScannerSE for scanning and processing of inked fingerprint cards. It is preconfigured specifically for "Secure Web Fingerprint Submission", or SWFT. It includes all of the features associated with the standard FormScannerSE, including "scan and entry" of fingerprint cards, assisted data entry, and ANSI/NIST compliant file creation and validation. It adds data formatting features that make it ready-to-go for file submission to the SWFT portal.

FormScannerSWFT is designed for one-at-a-time, assisted "scan and entry" processing of fingerprint cards, such as for manual data entry of previously scanned card batches. It can also be used for manual "rework" such as crop region adjustments.

FormScannerSWFT uses a template-driven workflow to support the processing of any card or form type. It automatically identifies the finger images present on the form, crop them, and perform quality analysis, segmentation, sequence checking, compression, and data structuring as ANSI/NIST-ITL Type-4 or Type-14, and (optional) Type-20 records. It utilizes Aware's AccuScan, NISTPack, and SequenceCheck SDKs.

The user interface implements workflow designed to enable the operator of the workstation to scan the form, make corrections, and manage the manual entry of the biographic data contained on the form. The section of the form containing the biographic data is displayed on the top half of the screen and the data entry boxes of the application are displayed on the bottom half of the screen. As the user moves the cursor to the selected data entry box, the scanned form pans and scrolls automatically in the top half of the screen so the original biographic data in typed or handwritten form is displayed prominently to assist keyed data entry.

A "rework station" equipped with FormScannerSE can be used to manually perform crop region adjustments, fix sequence errors, and perform data entry on previously scanned forms.

WHAT IS SWFT?

In 2010, the Under Secretary of Defense (Intelligence) (USD(I)) of the United States Director of Defense directed all DoD components to transition to electronic capture and submission of a full set of fingerprints in support of all background investigations by Dec. 31, 2013. This requirement extends to contractors cleared under the National Industrial Security Program (NISP). There are approximately 13,300 cleared facilities under the NISP. Of those, approximately eleven percent currently submit fingerprints electronically. Cleared facilities can begin using the Secure Web Fingerprint Transmission (SWFT) program to submit fingerprints electronically at any time.

SWFT is a web-based program that provides industry users the ability to securely transmit records directly from their records management systems to SWFT via secure web services. The process allows fingerprint images to be captured electronically, uploaded to the server where they are stored temporarily, and then released from the SWFT system to the Office of Personnel Management (OPM).

WorkbenchSuite™

A family of workstation applications for assisted review, analysis, repair, and processing of biometric images and transactions

WorkbenchSuite is a family of .NET workstation applications (available individually) designed to be used by an operator to analyze and repair or otherwise process digital records containing biometric images and data. Each targets a particular use case and implements workflow carefully designed to best assist analysts in their task.

FORENSICWORKBENCH
Assisted manual analysis and creation of compliant biometric records

SEQUENCEWORKBENCH
Analysis and repair of biometric fingerprint records containing sequence errors

CROSSLINKWORKBENCH
Analysis and repair of biometric records containing crosslinks

FACEWORKBENCH
Analysis and processing of candidates resulting from a facial biometric search

FINGERPRINTWORKBENCH
Analysis and processing of latent, livescan, and cardscan fingerprint searches.

APPLICATIONS

- Fingerprint recognition
- Face recognition
- Automated fingerprint identification services (AFIS)
- Automated biometric identification services (ABIS)
- Border management
- Defense and intelligence
- Law enforcement

ForensicWorkbench

Software application for assisted categorization, processing, and formatting of biometrics

ForensicWorkbench is a software application that utilizes several Aware SDKs for the categorization, processing, and standards-compliant formatting of biometric images and demographic data. It enables an analyst to organize a collection of biometric and demographic images and text files. The primary function of the application is the easy assembly of disparate biometric imagery and text into a standard-compliant data structure, such as ANSI/NIST-ITL 1-2013 (and earlier), FBI EFTS, and DoD EBTS.

ForensicWorkbench is designed to be used by an analyst to display and process biometric facial and fingerprint imagery and data. Facial images can be cropped to identify facial bounding boxes. The crop regions can then be labeled either as Frontal, Left Profile, Left 45 Profile, Right Profile, and Right 45 Profile. The operator may automatically extract frontal images from an input image or manually identify a face via the marking of the eye centers. For frontal images, Aware's PreFace is used to identify facial features and ensure compliance to an input frontal face specification. Input fingerprint images can be cropped to identify each finger (right and left thumb, index, middle, ring, little). Each finger can be labeled with its source and impression type (live scan, ink, rolled, plain) and its quality reported (Aware QualityCheck and NFIQ algorithms). The image storage format can be identified (RAW or WSQ).

Demographic data can also be entered. The demographic fields are fully configurable in accordance to the output ANSI/NIST specification. The entry of demographic data is supported through the display of image files and text files for operator review. Once data categorization and processing has been completed, the operator may generate an ANSI/NIST transaction. All data is validated by NISTPack prior to generation of the file.

APPLICATIONS

- Fingerprint recognition
- Automated fingerprint identification services (AFIS)
- Border management
- Defense and intelligence
- Law enforcement

Selection and processing of biometric images. The left side shows the raw biometric data yet to be processed. The right side shows biometric data the operator has selected for processing.

FEATURES FUNCTIONALITY

- Categorization of data into face, finger, iris, and documents
- Processing of finger, face, and iris imagery to label each image and sub-image with meta-data
- Measurement and reporting of image quality metrics for each sub-image,
- Generation of an ANSI/NIST-ITL-compliant output file
- Modification of the data within an existing EBTS file

Assembly of a transaction. This stage allows the operator both automated and manual options to analyze and process the biometric images so that they are of acceptable format and quality.

SequenceWorkbench™

A workstation application for review and repair of fingerprint sequence errors

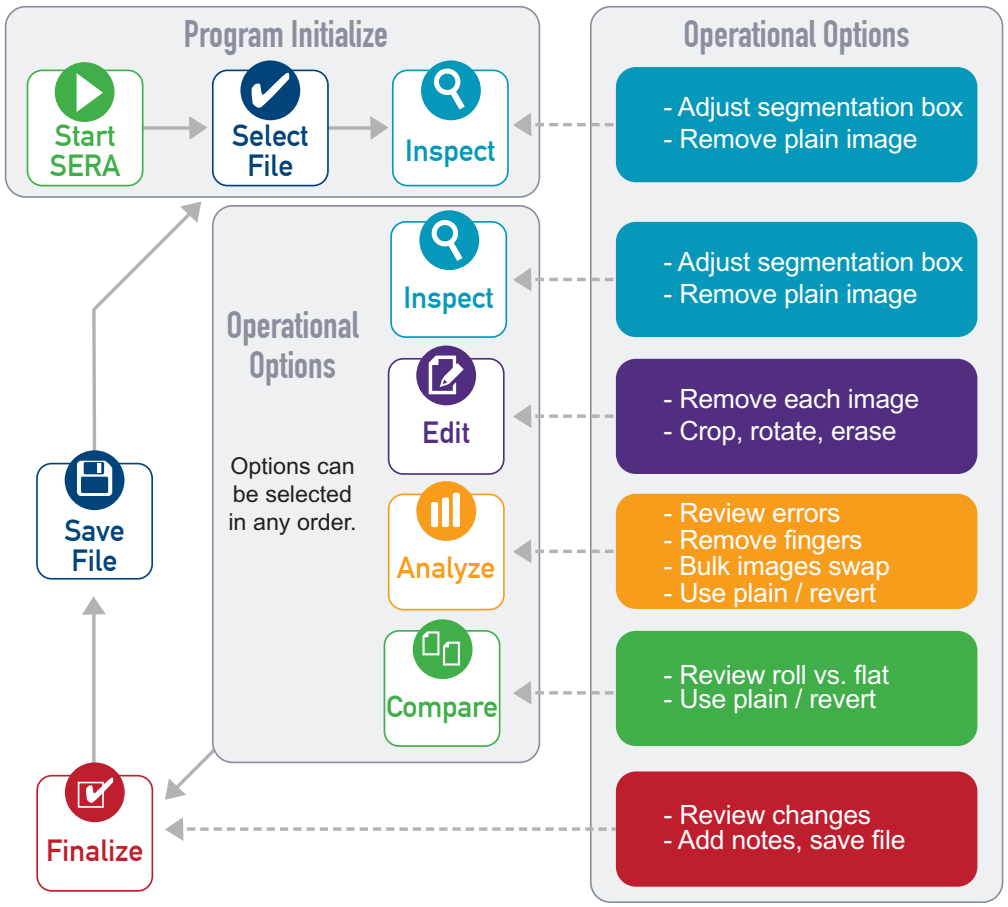
SequenceWorkbench is a software application designed to be used by an analyst to identify and repair sequence errors in fingerprint records. SequenceWorkbench will display and analyze the fingerprints

- Work with both Type-4 and Type-14 fingerprint images
- Edit individual fingerprint images (erase , rotate, adjust brightness and contrast)
- Compare fingerprint images (include zooming and panning)
- Remove individual fingerprint images
- Generate individual fingerprint images from multi-finger slap and plain images
- Reassign finger position values
- Mark fingers as missing
- Add notes to the caveat field (2.399)
- Process a series of transaction located in a directory
-

APPLICATIONS

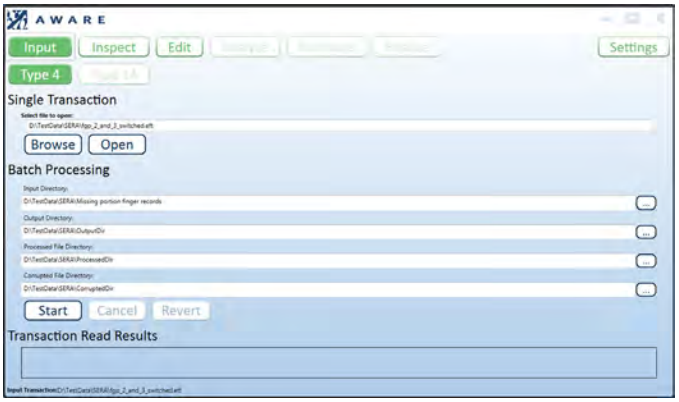
- Fingerprint recognition
- Automated fingerprint identification services (AFIS)
- Border management
- Defense and intelligence
- Law enforcement

SEQUENCEWORKBENCH WORKFLOW



INPUT

Using the Input Screen, the user submits whether they wish to process a single transaction or directory of transactions (batch processing). Errors or warning encountered reading the transaction will be reported.

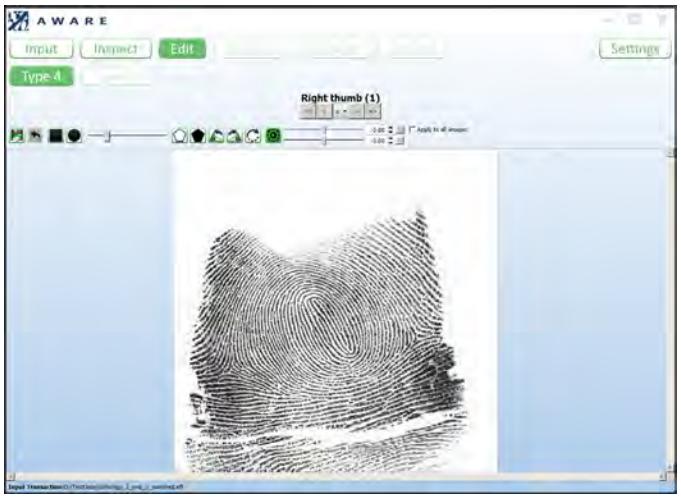


INSPECT

The Inspect Screen gives an original view of the images in the transactions in a tenprint card layout. It allows user to remove plain thumb and slap images. This screen also shows the segmentation of the multi-finger plain images. The user is given the ability to adjust or reset the segmentation boxes.

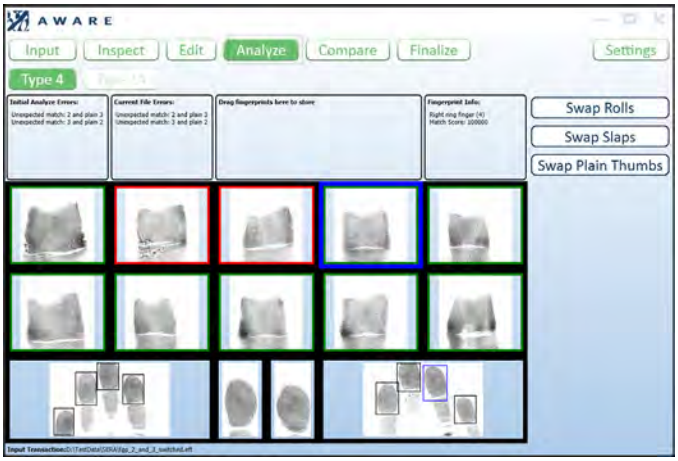
EDIT

A user may use the Edit Screen to erase, rotate, crop, adjust brightness and contrast fingerprint images before they are analyzed. The program can be configured so that each image in the transaction must be reviewed on the edit screen before continuing on to the other screens.



ANALYZE AND REPAIR

Results of the sequence check are shown using the Analyze Screen. Prints that have errors are highlighted with specified colors. Errors are reported as text in status boxes. The user is able to move prints to different position to correct sequence errors. They can also remove the prints (by placing it in the tray) or do bulk operation like swapping rolls, slaps or plain thumbs. Double click on an image would navigate to compare screen, and hence user can perform individual comparison between the selected image and its corresponding plain.

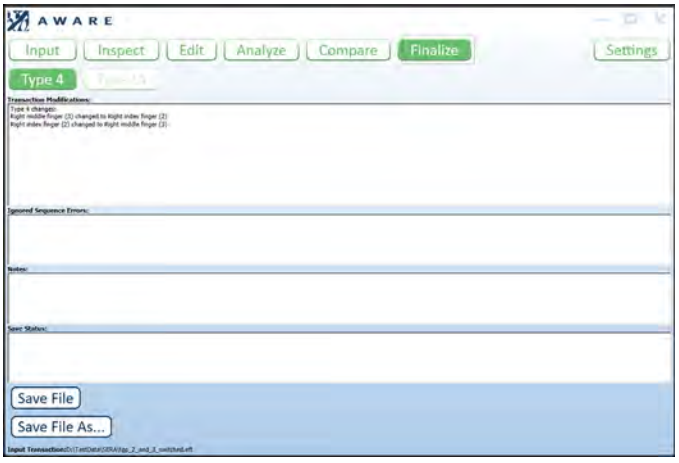


COMPARE

The user may use the Compare Screen to view two prints simultaneously. The prints can be viewed in 'Sync' mode where the roll will be displayed on the left side and the corresponding plain image will be shown on the right. The sync mode can be disabled and each print can be viewed against any other print. In addition, a user can replace a roll impression with the corresponding plain impression on this screen. If there is sequence error with the print that is currently be review, the user can choose to ignore the error and enter a reason for ignoring. This reason will be placed in the finalized transaction in the caveat field.

FINALIZE SCREEN

The Finalize Screen provides a summary of the changes to the transaction and a list of errors that were ignored. On this screen you are also given the ability to add in notes that will appear in the caveat field.



SETTINGS SCREEN

The Settings Screen allows user to set various options for program displays and behaviors. Reset buttons for resetting color scheme and default sequence check cutoff scores setting.

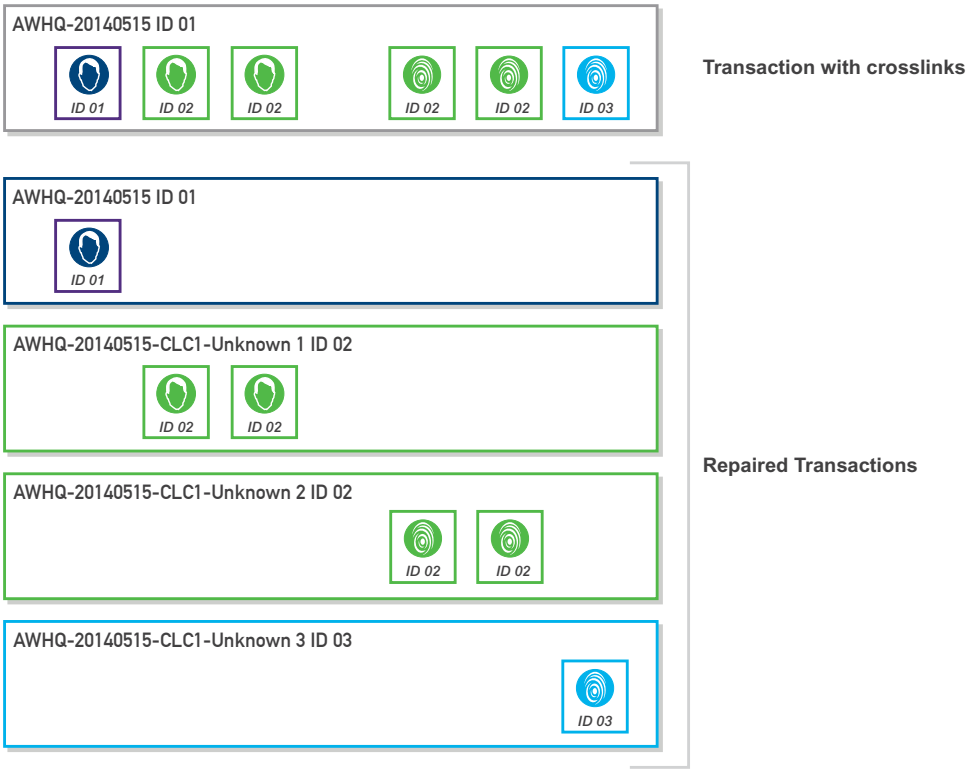
CrosslinkWorkbench

A workstation application for detection, analysis, and repair of biometric crosslink errors

CrosslinkWorkbench is an application that utilizes several Aware SDKs for assisting with identifying and repairing of crosslink errors in ANSI/NIST ITL transactions. Crosslinks are biometric records that erroneously contain data from different individuals. CrosslinkWorkbench uses the concept of "assigned identities" to help the user repair crosslinks. An identity is defined as a grouping of biometrics that has come from the same person. In the diagram below, the original transaction has biometrics from three different individuals. Using the comparison tools in CrosslinkWorkbench, the examiner assigns identities to the each of the biometrics. For each modality (e.g. face, finger, etc.), CrosslinkWorkbench places all biometric images with the same identity into a single transaction when generating the output. If all biometrics in a transaction have the same identity as the original transaction, nothing will be written.

FEATURES AND FUNCTIONALITY

- Display of images from Type-4, 7, 10, 14, 15, 16, 17, and 20 records types as they appear in the transactions
- Display all the images of a single type on the screen so they can be compared (with pan and zoom).
- Assignment of identities to transactions and images so that corrected transactions can automatically be created.
- Assignment of output targets to images so specific images can appear in specific output transactions
- Deletion of biometrics from transactions
- Use of assigned identities and/or output targets to modify existing transactions and create new transaction that represents the crosslink repair operation
- Visually display the results of crosslink repair
- Create a text report of a crosslink repair



A TYPICAL WORKFLOW IS OUTLINED BELOW:

1. On the ***Input*** screen set directories and click the Start button
2. Analyze biometrics on ***Compare*** screen
3. Assign biometrics that come from the same individual to the same identity
4. Create additional identities if needed (i.e. there are more individuals than transactions)
5. If biometrics of different modalities, or images that are located in different transactions, need to be placed into a single output transaction, create a new output target and assign to those biometrics
6. If any images need to be removed, assign them to the ***Delete*** Identity
7. Review the output images with desired transaction under Review screen.
8. Result summary is displayed under ***Finalize*** screen where user can click on 'Save' button to generate corresponding transactions in designated folders. Expected result text file is also generated at root directory as well.

APPLICATIONS

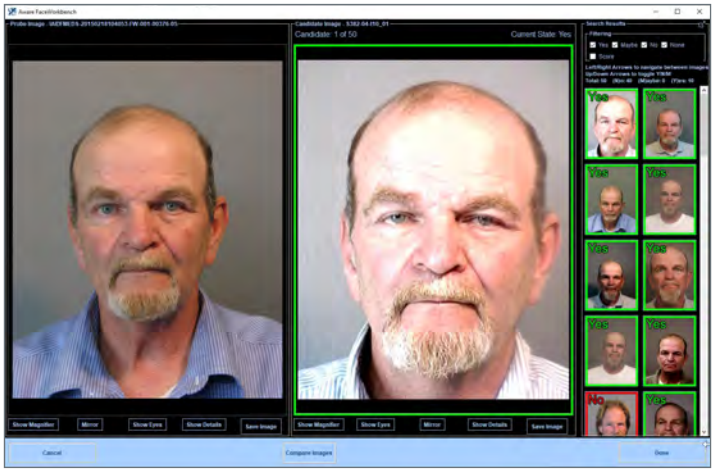
- **Fingerprint recognition**
- **Automated fingerprint identification services (AFIS)**
- **Border management**
- **Defense and intelligence**
- **Law enforcement**

FaceWorkbench

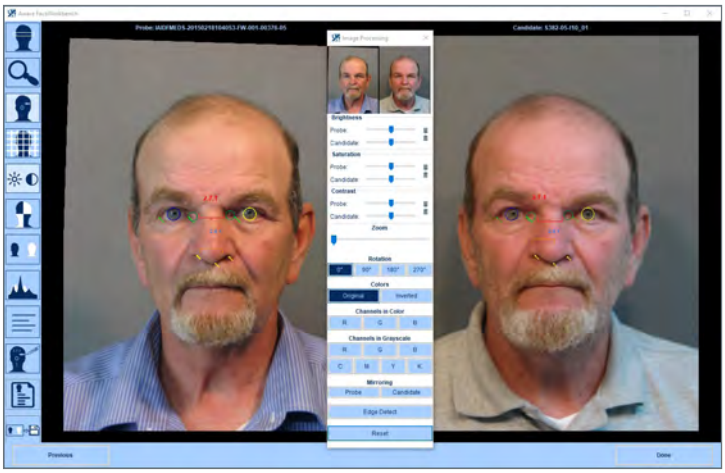
A workstation application for forensic analysis and processing of facial biometric search results

FaceWorkbench is a client application used by biometric examiners to perform facial reviews in various biometric operation workflows, including 1:N, 1:1, and training. It is distinguished by its thoughtful and forward-looking incorporation of current and emerging guidelines and best practices resulting from recent work in the forensic community within the US Government, international standards bodies, and independent forensic associations.

FaceWorkbench integrates examination-based workflows for comparison and training enabling a facial examiner to work in the most efficient way possible while enforcing these current and emerging guidelines and best practices in a supportive role. FaceWorkbench also incorporates numerous ease-of-use features for the facial examiner so critical tools and resources needed for an examination are readily available and effective to use with minimal effort.



Search results review



Comprehensive image manipulation toolset

APPLICATIONS

- Border management
- Defense and intelligence
- Law enforcement

FEATURES & FUNCTIONALITY

- Single or bulk facial match submissions
- Comprehensive examination workflow in one cohesive application
  - queue management
  - image calibration
  - intense 1:1 review
  - reporting
- Reduces or eliminates tedious processes
- Provides useful image analysis features
- Instant access to operational guideline documents
- In-application reporting
- Integrated training mode
- Easy screen capture and terminology references
- Automated report generation

For example, the features of the facial images of the probe and candidate are automatically located and used to align the images (with a manual eye location override if needed to better align the images.) There are advanced image enhancement functions, including swipe bars, color manipulations, and other enhancements, as well as a synchronized, configurable magnifier. Comparison tools allow the images to be overlaid and blended, split, stacked, and checkered.

A key feature of FaceWorkbench is its integration of forensic facial analysis best practices and guidelines into the operational workflows or examiner training sessions. Guidelines such as those drafted by FISWG (www.fiswg.org) or determined by the agency can be integrated prompting the examiner to follow defined operational best practices and keep track of which analyses have been performed. Agencies then realize tighter integration of best practices into the training and operational context.

Another key feature is its automated report generation, which serves to document all the steps taken and best practices followed by the examiner that led to their conclusion. The reports save examiners' valuable time, while making their evidence more clear and informative in a legal procedure.

FaceWorkbench used with AwareABIS™

AwareABIS™ is an Automated Biometric Identification System (ABIS) used for large-scale biometric identification and deduplication, with support for fingerprint, face, and iris modalities. Its highly modular architecture allows it to be configured and optimized for either civil or criminal applications.

AwareABIS leverages BioSP™ (Biometric Services Platform), Aware's market-leading workflow and integration server to achieve unsurpassed configurability and ease-of-integration. It has the flexibility to utilize Aware's high-performance, NIST-tested Nexa™ face, fingerprint, and iris matching algorithms, as well as top-tier fingerprint algorithms from 3rd-party providers. Together, these features make it the best ABIS on the market not only for extreme configurability but for prevention of vendor lock-in.

AwareABIS is also fast, scalable, and reliable, using Astra™, an advanced cluster computing platform to perform searches against millions or tens-of-millions of records.

Thorough image analysis

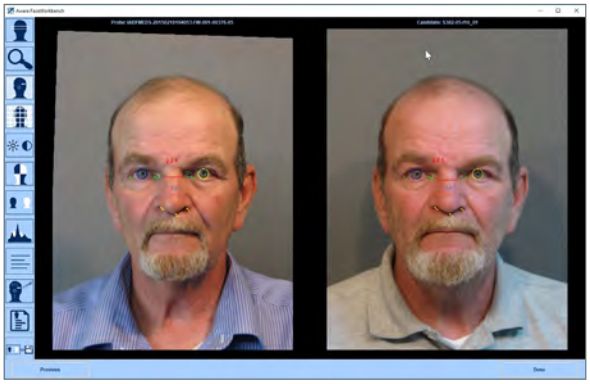


Image annotation tools

Detailed search results analysis

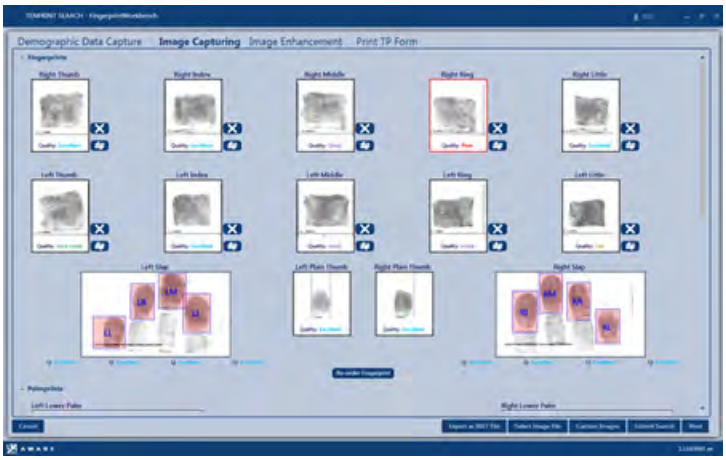
Automated generation of reports

FingerprintWorkbench™

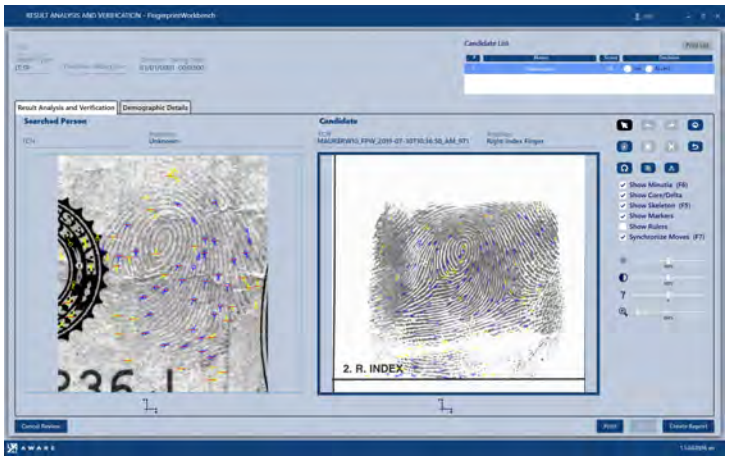
A workstation application for forensic analysis, processing, and reporting of biometric fingerprint evidence, comparisons, and search results

FingerprintWorkbench is a workstation application used by fingerprint examiners to perform latent fingerprint examination and tenprint match results review and reporting. Used as part of AwareABIS, it provides useful, intuitive tools and workflows that help the examiner to complete their tasks more effectively and more efficiently, with support for 1:1 comparison and 1:many search.

Distinguished by its forward-looking, intuitive design and comprehensive capability set, FingerprintWorkbench offers workflows highly optimized for efficiency and high performance as well as configurable input (live scan and card scan format options) and output (print card format). It does so in part by incorporating useful examination tools–readily available with minimal effort–directly into the workflows, while also enforcing best practices. POWERFUL MATCHERS FROM



Tenprint search



Latent search results analysis and verification

FEATURES

- Comprehensive search workflows
  - Tenprint to tenprint or latent
  - Latent to tenprint, palm, or latent
- Livescan, print card, file image, and biographics submission
- Management of search queues
- Appendix F certified card scanning, formatting, output
- Several supported workflows
  - Latent and tenprint registration
  - Queue management
  - Latent match charting
  - Decision verification
- Image processing features
  - Histogram (brightness, contrast, equalization, etc.)
  - Sharpness
  - Ghost removal
- Minutiae processing
  - Add/delete
  - Quality filtering
- Match results verification
  - Minutiae pair mating
  - Annotation of final decision
- Latent match charting
  - Assists in courtroom presentation of match results

AWARE OR 3RD PARTIES

Nexa|Fingerprint™, Nexa|Face™, and Nexa|Iris™ SDKs include biometric search algorithms for fingerprint, facial, and iris recognition. Unlike other ABIS, AwareABIS™ has the ability to utilize biometric algorithms from other suppliers.

Fingerprint transactions can be generated from disk or by using live scan collected images, as well as those scanned using a flatbed scanner. Both capabilities are natively supported in FingerprintWorkbench using Aware's time-tested LiveScan API and AccuScan products. LiveScan API supports over 50 legacy and currently available

fingerprint devices. AccuScan provides certified flatbed scanning using configurable card layouts allowing FingerprintWorkbench to scan most common card formats. The FingerprintWorkbench interface also includes biographic data entry and rendered tenprint card display and printing.

FingerprintWorkbench workflows provide a linear "walk-through" of each examination process. The operator may submit a new latent or tenprint search, or review prior search results from the AFIS. Tools are provided for analysis of ridge flow and minutiae type annotation and placement. A key feature of FingerprintWorkbench is its rich collection of image analysis and exploitation tools. These include brightness, contrast, and gamma tools as well as frequency analysis tools to emphasize or minimize repeating patterns within the image.

FingerprintWorkbench also provides tools for the analysis of pre-calculated (e.g. by an AFIS) features (core, delta, and minutiae type, location, direction, ridge flow), as well as the ability to manually identify and set these features. A tool to check the validity of matching minutiae pairs is also provided. Each individual encoding feature can be displayed or turned off to assist the image analysis process.

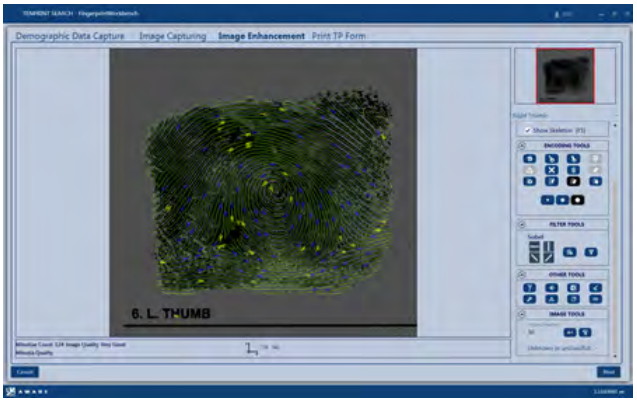
FingerprintWorkbench used with AwareABIS™

AwareABIS™ is an Automated Biometric Identification System (ABIS) used for large-scale biometric identification and deduplication, with support for fingerprint, face, and iris modalities. Its highly modular architecture allows it to be configured and optimized for either civil or criminal applications.

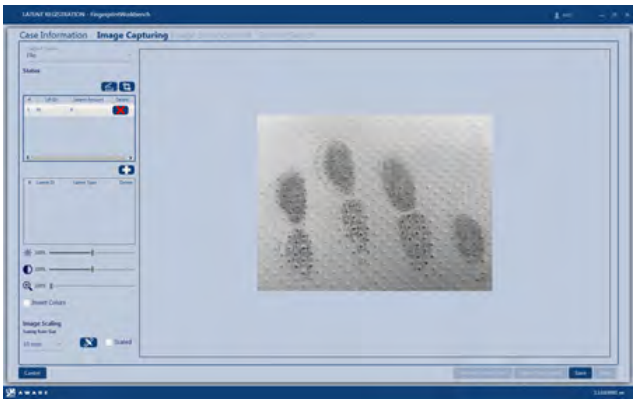
AwareABIS leverages BioSP™ (Biometric Services Platform), Aware's market-leading workflow and integration server to achieve unsurpassed configurability and ease-of-integration. It has the flexibility to utilize Aware's high-performance, NIST-tested Nexa™ face, fingerprint, and iris matching algorithms, as well as top-tier fingerprint algorithms from 3rd-party providers. Together, these features make it the best ABIS on the market not only for extreme configurability but for prevention of vendor lock-in.

AwareABIS is also fast, scalable, and reliable, using Astra™, an advanced cluster computing platform to perform searches against millions or tens-of-millions of records.

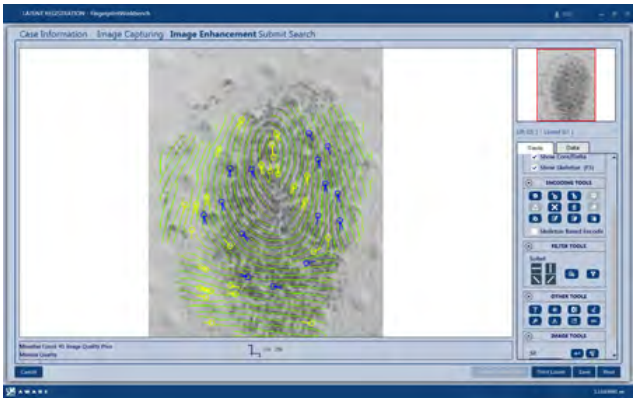
Live scan / card scan fingerprint enrollment



Extensive and intuitive analysis tools



Latent fingerprint enrollment



Latent markup and enhancement

BioComponents™

Software components for biometric enrollment

BioComponents comprise Aware's biometric enrollment application framework, and include a family of independent software components. Each is designed to enable rapid implementation of a .NET or browser-based biometric enrollment application with a high degree of configurability in terms of functionality and macro-workflow.

Each BioComponent is modular, independent, and self-contained. They run in any modern browser and each operate independently and in concert, with each performing a specific biometric task. Each BioComponent has its own user interface, and performs all workflow and tasks required for biographic data capture and validation, biometric image capture and processing, hardware abstraction, quality assurance, and networking.

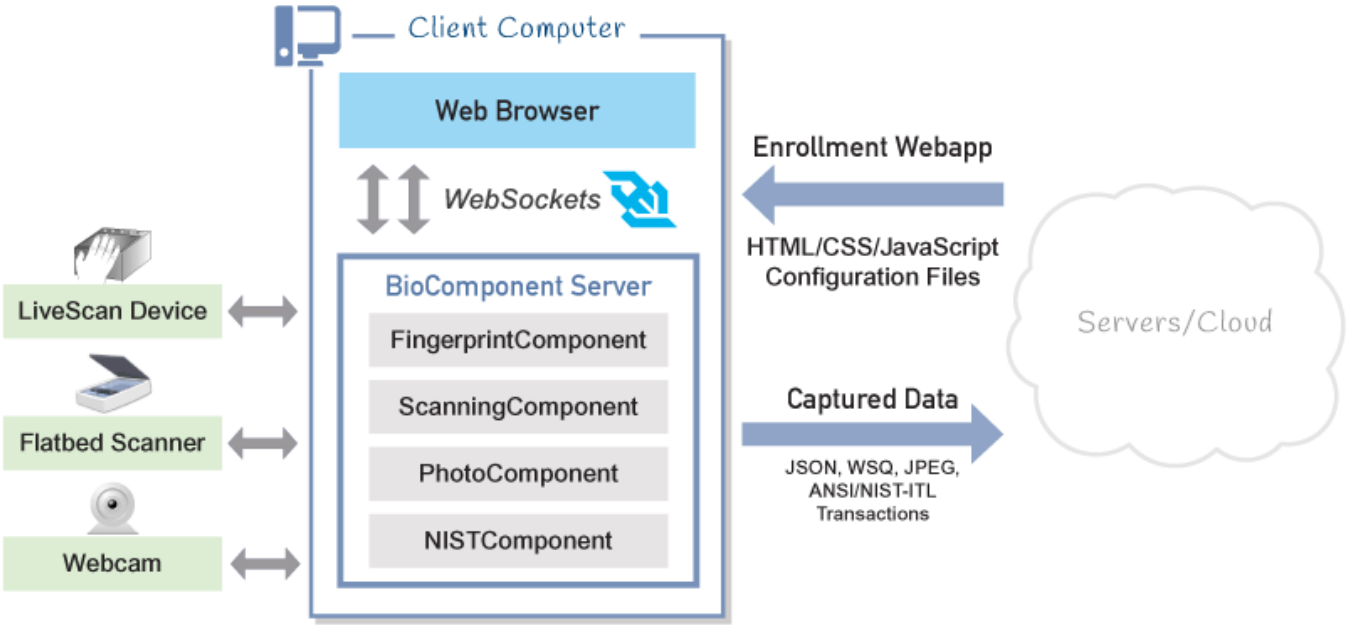
BioComponents are each provided with a proven reference "workflow". The workflows can be configured or completely replaced. They run within a customer-designed UI allowing a custom application to be designed according to specific look and feel and business rules.

All BioComponents utilize APIs from Aware's well-established and field-proven SDKs for underlying biometric functionality. They are designed to

BioComponent	Functionality
FingerprintComponent	Fingerprint capture and scanner abstraction
PhotoComponent	Face capture and camera abstraction
ScanningComponent	Scanning of fingerprint cards and other forms
PrintingComponent	Printing of fingerprint cards and other forms
NISTComponent	Biographic and textual data entry and formatting, NIST compliance checking, and submission

APPLICATIONS

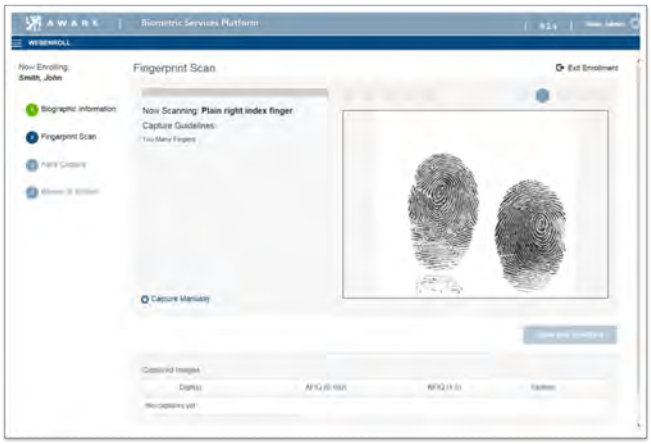
- Fingerprint recognition, face recognition, iris recognition
- Automated fingerprint identification services (AFIS)
- Automated biometric identification services (ABIS)
- Border management
- Citizen ID and voting systems
- Defense and intelligence
- Law enforcement



eliminate the need to program directly against Aware SDKs, but they include their own APIs to allow communication and data sharing with the main application. BioComponents are included in Aware's Universal Registration Client (URC™) .NET enrollment application and WebEnroll, a browser-based biometric enrollment and data management solution.

BioComponents are particularly well-suited for supporting multiple different biometric enrollment applications from a single platform, with each having some different functionality requirements and constraints. Using BioComponents provides common capabilities, maintenance, and support, and yet enables simple configuration variations to accommodate the unique workflows of each application.

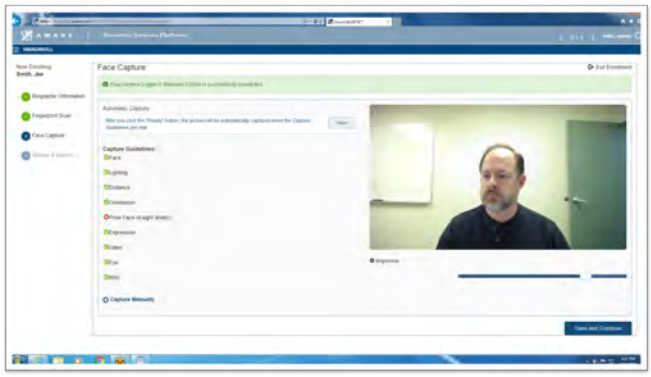
FingerprintComponent



Fingerprint Component implements libraries from three Aware SDK products: LiveScan API, SequenceCheck, and Aware WSQ1000. It includes its own user interface and offers a variety of workflows to perform capture. It performs:

- **Real-time quality analysis and autocapture of slap images**
- **Abstraction of live scan hardware peripherals**
- **Segmentation of slap fingerprint images**
- **Sequence checking**
- **Post-capture quality analysis and scoring**
- **Highly-optimized, FBI-certified WSQ image compression (500 ppi images)**
- **Highly-optimized, FBI-certified JPEG 2000 image compression (1000 ppi images)**

PhotoComponent



PhotoComponent is used to automatically capture biometric facial images according to U.S. and international biometric standards (e.g. ISO/IEC 19794-5). It includes libraries from the PreFace. It has its own user interface and performs:

- **Real-time quality analysis and autocapture of facial images**
- **Post-capture quality analysis of facial images**
- **Post-capture image processing (rotate, scale, crop, optimize)**
- **Camera abstraction**
- **Camera operation (zoom, brightness, color balance, shutter)**
- **PhotoComponent supports consumer-grade cameras, webcams, and industrial cameras from many different vendors (see PreFace).**

ScanningComponent

ScanningComponent is used to scan forms such as inked fingerprint cards, and incorporates libraries from the AccuScan SDK product. It performs:

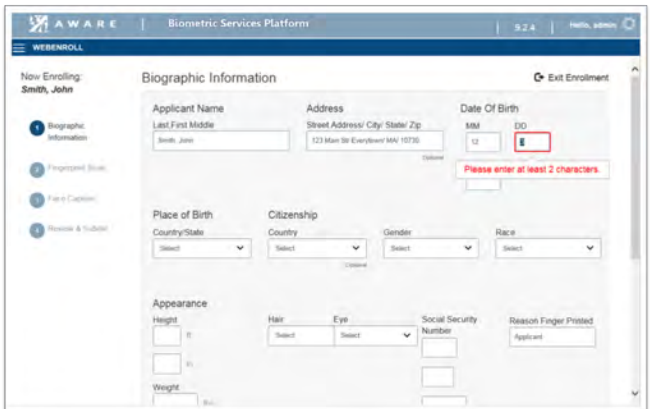
- **Flatbed scanner abstraction, with many FBI-certified scanners supported**
- **Compliance with FBI EBTS Image Quality Specification.**
- **Cropping of individual fingerprint images from a form in preparation for compression and formatting.**

PrintingComponent

PrintingComponent is used for printing fingerprint images on cards and forms with quality sufficient for FBI-certification. It utilizes libraries from Aware NISTPack and AccuPrint SDKs. Functionality includes:

- **Parsing of fingerprint images from transactions, such as EFTS**
- **Decompression of fingerprint images**
- **Mapping of text and images to correct location on the form**
- **Printing of card graphics such as lines and labels**
- **Generation of 1-bit dithered image to simulate grayscales**
- **Creation of a post-script or PCL-based image and sending to printer.**

NISTComponent



NISTComponent has access to the data set that the other components build up, and also has the ability to save the currently entered data set or to alternatively replace the current data set with data from another saved data set. PackagingComponent can:

- **Text-based biographic data entry**
- **Save the current data set to a standards-compliant file (FBI EBTS or other)**
- **Replace the current data set with a set selected**
- **Build a transaction from the current data and submit it via SMTP, or web service to BioSP**
- **Verify entire transactions**

NISTComponent can then save or submit the updated transaction.

Inquire™

Advanced text search and identity analytics SDK

Inquire™ is a software development kit that performs fuzzy text-based filtering, searching, matching, and linking functions towards discovery of useful information in identity data. Analysis of text-based identity data is naturally complementary to biometric verification and identification, and Inquire is optimized for processing and analysis of data that includes biometrics.

Inquire provides many advanced text matching comparison algorithms and flexibility in how matching algorithms behave (e.g. thresholds, data definitions). It can be used to perform advanced analysis of text-based identity data for several useful investigative applications including data analysis and quality assurance, data integration, identity resolution, and link analysis. Inquire is fully scalable, with infrastructure that automatically determines processing resources and optimizes their utilization.

FUNCTIONALITY

- Identity data quality analysis and cleanup
- Data integration
- Identity resolution
- Link analysis for relationship discovery
- Probabilistic (fuzzy) text search and match
- Name and address matching
- Biometric search pre-filtering
- Soft biometrics

FEATURES

- Quantitative similarity scoring and ranking
- Customizable dictionaries and link rules
- Well-designed, easy-to-use APIs
- Fully scalable and extensible
- Portable between client and server hardware and OS, database platforms
- C, .NET Assembly, and JNI interfaces, error codes, sample program source code

FUZZY NAME AND ADDRESS MATCHING

Inquire performs comparisons between text fields in identity records, such as names, addresses, and other biographic identity data. It can be configured to recognize common variations in spellings and formats to improve the performance and reliability of identity search and filter processes.

NAME VARIANTS
Brian ≈ Bryan
Sara ≈ Sarah

NICKNAMES
Jack ≈ John
Bobby ≈ Robert

SPECIAL CHARACTERS
Mueller ≈ Müller
OCallahan ≈ O'Callahan

PHONETIC SIMILARITIES
Mohamed ≈ Muhammad
Geoffrey ≈ Jeffrey

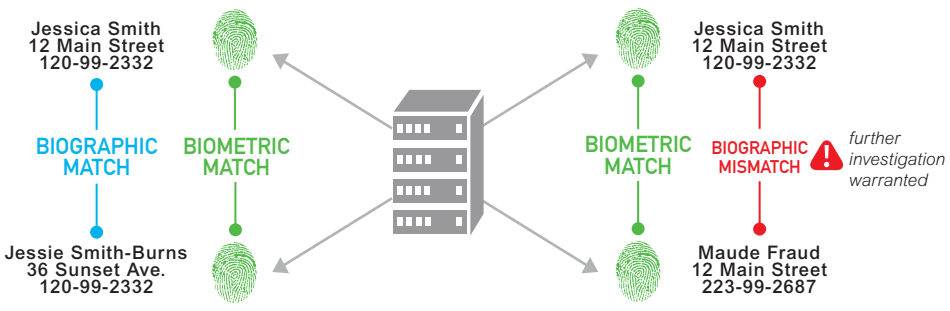
Washington ≈ Washimgton

MISSPELLINGS
Albuquerque ≈ Albequrque

NAME CHANGES
Laura Smith ≈ Laura Smith-Jones

BIOGRAPHIC DATA MATCHING

Inquire can be used to identify potentially fraudulent identity information in a biometric database based on the content of multiple fields and attributes. For example, a name that changes due to marriage or an address that changes due to a move can be noted as a biographic match, while an identity demonstrating potentially fraudulent content can be automatically highlighted as requiring further investigation.

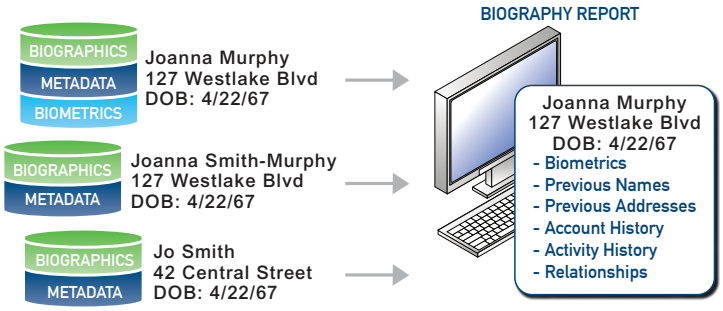


BIOMETRIC SEARCH FILTERING

Inquire can be used to pre-filter or post-filter a biometric search based on fuzzy matching of text-based fields, including biographic information or "soft biometrics" such as hair color, eye color, height, weight, and age.

IDENTITY DATA ANALYSIS AND QUALITY ASSURANCE

Assuring the quality and integrity of identity data is vital to its effective use, and so should be performed as an integral part of an identity system. Inquire can be used to assess the quality and integrity of identity data, including data that contains biometrics. It can be used to detect errors such as typos, misspellings, as well as biometric false matches, non-matches, and crosslinks.

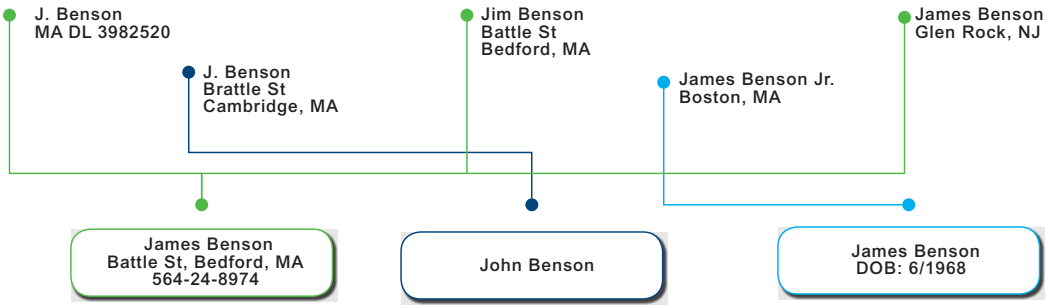


APPLICATIONS

- Data quality analysis and repair
- Identity record search
- Fraud prevention and detection
- Biometric identification pre/post-filtering
- Know your customer / know your employee

DATA INTEGRATION AND IDENTITY RESOLUTION

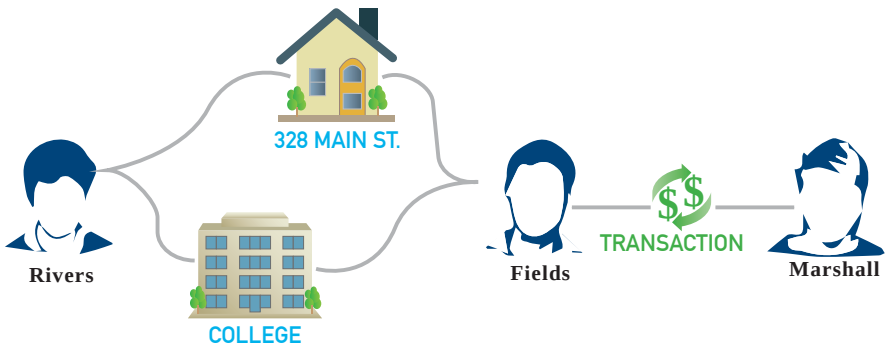
Inquire performs integration of identity data records across databases, linking attributes and encounters associated with a particular individual to a single identity record. Inquire uses fuzzy text comparison algorithms to link and merge data records, and accommodates artifacts such as misspellings, name variations, and address changes. Once the data sources are resolved, a user can perform queries and generate a comprehensive multidimensional view of an individual's biographic information and activities.



LINK ANALYSIS FOR RELATIONSHIP DISCOVERY

Inquire performs link analysis that visualizes identity data to reveal non-obvious relationships between individuals and other entities.

QUERY	SSN	LastName
Primary	198-30-1093	Rivers
Secondary	388-20-2001	Marshall

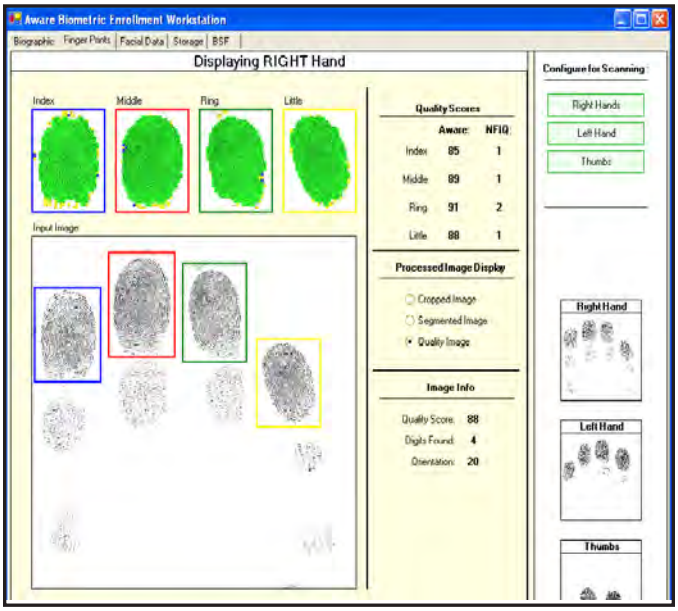


LiveScan API

Fingerprint autocapture, quality assurance, and scanner abstraction

Fingerprint Autocapture, Quality Assurance, and Scanner Abstraction

LiveScan API is an SDK that provides fingerprint capture device abstraction though a common API. It supports over forty single finger, multi-finger and palm capture devices and is designed to allow an application to support any of these devices with no changes to the application code. It is ideal for fingerprint identification and verification applications where multiple high-quality, standards-compliant fingerprints must be collected within strict time constraints, and where it is desirable to utilize the same enrollment application with different hardware devices over time or within a system.



REAL-TIME IMAGE ANALYSIS AND CAPTURE LOGIC

LiveScan API provides capture logic that helps ensure true device abstraction. It is a programmable, configurable logic layer that allows an application to make autocapture decisions independently and without influence of the API or firmware of the device. It enables a biometric enrollment application with automated fingerprint capture and quality assurance. It performs real-time quality checks on finger images to ensure compliance and maximum quality before a final image is taken, dramatically improving overall capture speed. LiveScan API performs the following processes in real time prior to final image capture:

- **Fingerprint segmentation and bounding box definition**
- **Ridge flow-based image quality scoring**
- **Leftness and rightness detection and measurement**
- **Finger angle measurement**
- **Missing finger detection**
- **Finger on platen edge detection**

Real-time analysis of the preview mode data greatly reduces the likelihood that the captured image must be recaptured because it fails post capture quality analysis. By setting programmable quality targets and thresholds, each slap or individual fingerprint image is captured automatically only when it satisfies the above requirements. In doing so, LiveScan API substantially improves capture time and workflow efficiency, enabling collection of a complete set of ten flat fingerprints in as little as ten seconds.

CAPTURE DEVICE ABSTRACTION

LiveScan API abstracts the device interface layer from the application logic and to provide optimal quality of capture without undue dependence on the device. LiveScan API provides abstraction of most market leading fingerprint scanning devices, including live scan, single and dual finger devices, and capacitive sensors. Support for new hardware is added in subsequent revisions of the SDK as they become available. A list of supported devices is available upon request.

USE WITH OTHER PRODUCTS

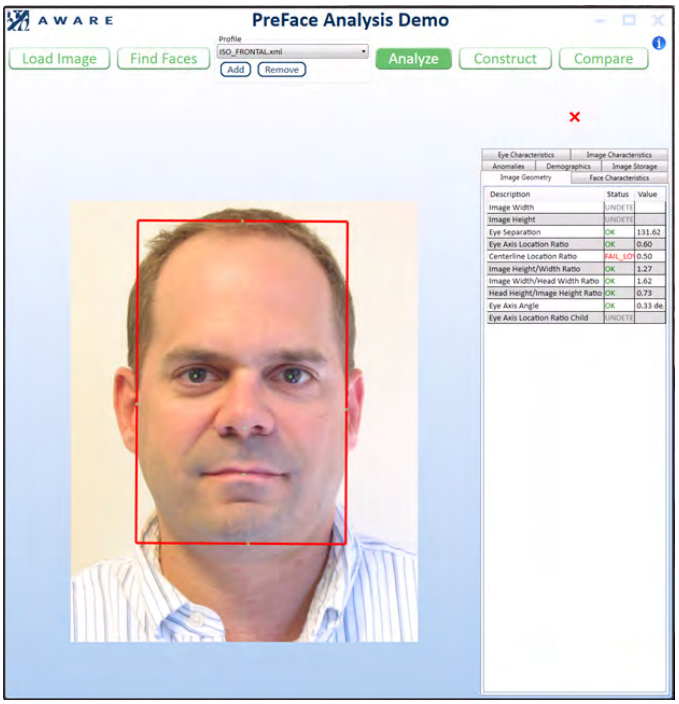
LiveScan API output, along with biographical data, can be forwarded to Aware's NISTPack software libraries to create FBI- and/or NIST-compliant Type-14 EFTS fingerprint records, acceptable for civil background check submissions.

PreFace™

Biometric facial image autocapture, quality assurance, liveness detection, and camera abstraction

PreFace is an SDK that automatically captures and analyzes biometric facial images in order to maximize their quality and matchability. It can enable a biometric enrollment application to automate the facial image capture process and also ensure that enrolled images comply with ISO standards or backend processing system and are of sufficient quality to perform biometric matching.

PreFace integrates with the camera to perform analysis of the live facial image stream or video. Once basic quality criteria are met, PreFace triggers the camera to take a full-resolution image. Following capture, PreFace performs a thorough image analysis, which reports image geometry, non-compliant features, and spoof attempts. Scaling, rotation, and cropping of the image is performed to meet highly configurable targets and thresholds. These thresholds are derived from the ISO/IEC 19794-5 standard for biometric facial image quality. Results are reported to the user. PreFace also includes a robust face finder, able to locate multiple faces in a single frame in both still shots and video.



FEATURES & FUNCTIONALITY

- Automates photo capture and improve operational efficiency of the capture process
- Maximizes the visual quality of biometric facial images for human comparison
- Improves matching performance by screening non-compliant images upon capture
- Performs automatic “rotate, scale, crop” geometrical corrections
- Notifies operator of pre- and post-correction non-compliant features
- Performs liveness detection / spoof detection in active (user interaction) and passive modes
- Creates compliant ISO/IEC 19794-5 biometric records
- Ensures compliance with ANSI/INCITS 385-2004 and ISO/IEC 19794-5 standards for biometric facial image quality
- Integrates market leading digital cameras, web cams, and industrial cameras, including new cameras as the arrive on the market
- Performs estimation of demographic qualities: age, race, and sex
- Estimates pose: yaw, pitch, and roll
- Detects and analyzes multiple faces in an image
- Optimizes brightness and contrast to compliance (include a screen shot of before and after)
- Identifies key facial feature coordinates including eyes, nose, mouth and chin
- Compresses image to targeted file size or quality level
- Supports multiple image formats: PNG, BMP, TIF, JPEG, JPEG 2000, RAW-8, RAW-24

APPLICATIONS

- Facial recognition
- Face finding
- Automated Biometric Identification Systems (ABIS)
- Biometric authentication
- Liveness detection / spoof detection
- Fraud prevention
- Citizen ID and voting systems

Liveness Detection

Active and passive modes
Face finding in video
Blink detection
Mobile-optimized

Face Characteristics

Pose Angle Yaw
Dynamic Range
Brightness
Saturation
Smile

Eye Characteristics

Eye Contrast
Eye Obstructed (Left or Right)
- Glasses Frames
- Hair
- Closed Eye
- Eye Valid
Off-angle Gaze
Red-eye

Image Characteristics

Number of Image Channels
- Background
- Gray
- Uniformity
- Clutter
- Type
- Color Balance
- Pad Type
Conditional Padding

Anomalies

Illumination Asymmetry
Facial Shadows
Focus
Sharpness
Unnatural Skin Color
Glasses
Glasses with Dark Lenses
Glasses Glare
Glasses with Heavy Frames
Forehead Obstructed

Image Geometry

Image Width
Image Height
Eye Separation
Eye Axis Location Ratio
Centerline Location Ratio
Image Height/Width Ratio
Image Width/Head Width Ratio
Head Height/Image Height Ratio
Eye Axis Angle

Demographics

Estimated Age
Gender-Female
Gender-Male
Race-White
Race-Black
Race-Asian

Image Storage

JPEG Quality Level
File Size
JPEG2000 Compression Ratio
Within ROI
Outside ROI
Image Format

SDK FEATURES

- Fully featured C Language API
- C#/.NET wrappers
- Example programs with source
- Java Native Interface support
- Android and iOS support (PreFace Mobile)

CAMERA API

PreFace includes “Camera API,” which serves to abstract camera hardware and integrate software-driven autocapture with a variety of consumer-grade digital cameras, webcams, and industrial cameras. It is designed to greatly simplify the task of integrating a facial image camera into a photo capture application. Camera API provides a method by which to support many different cameras within a single application; program once, and use many. Support for new cameras is added in subsequent revisions of the SDK as they become available. Camera API enables a biometric application to operate equivalently with a variety of devices over time or within the same system. Cameras are also tested and submitted for approval by the GSA for use in FIPS 201 compliant “PIV” U.S. government employee credentialing systems. An up-to-date list of cameras supported by Camera API is available from Aware upon request.

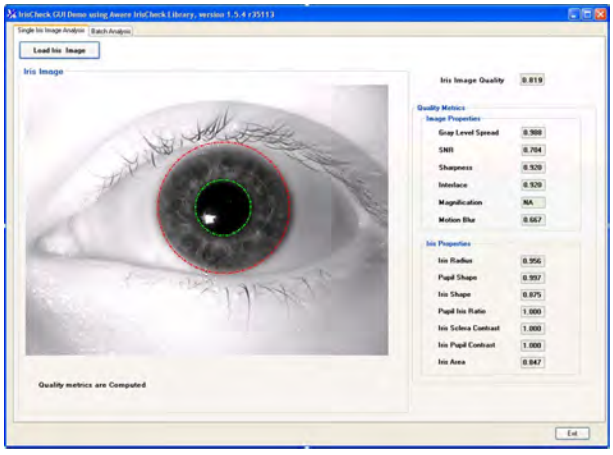
IrisCheck™

Biometric iris image quality analysis and iris camera abstraction

IrisCheck™ is a software development kit (SDK) used for automated quality analysis and compliance assurance of biometric iris images. It performs advanced analysis and image processing to assign quality scores, detect non-compliant features, and perform JPEG 2000 compression according to the ISO/IEC 19794-6 standard. IrisCheck operates equivalently with different iris cameras from different vendors, enabling an enrollment application to operate independently from cameras and matchers.

IrisCheck performs several analyses to assign a quality score to each image based on the following characteristics derived from ISO/IEC 29794-6:

- Iris characteristics and geometry
- Pupillary dilation
- Iris eccentricity
- Pupil/iris displacement ratio
- Eyelid occlusion
- Off-axis gaze angle
- Contrast
- Usable iris area
- Resolution (e.g. iris radius in pixels)
- Anomalies and non-compliant features
- Degree of focus blur
- Degree of motion blur
- Patterned contact likelihood
- Degree of shadow attenuation



IrisCheck SDK reference application showing quality analysis of iris image according to ISO/IEC 29794-6

FEATURES & FUNCTIONALITY

- Performs quality analysis and compliance assurance
- Helps automate iris image capture
- Automatic iris segmentation
- Improves capture process efficiency
- Image output as ISO 19794-6 objects or "Kind" images
  - Kind 1: Uncropped
  - Kind 2: VGA
  - Kind 3: Cropped
  - Kind 4: Cropped and masked
- Ensures compliance of iris images with
  - NIST IREX I Report (NISTIR 7629)
  - NIST IREX II Report
  - ISO/IEC 19794-6 data interchange format standard
  - ISO/IEC 29794-6 iris quality standard (draft)
- Assigns quantitative quality scores that correlate to matching performance

IrisCheck applies advanced image processing algorithms to optimize the image for matching and ensure compliance:

- Specularity removal
- Pupil segmentation
- Iris segmentation
- Parametric curve fitting
- Eyelash detection

APPLICATIONS

- Iris recognition
- Automated Biometric Identification Systems (ABIS)
- Biometric authentication
- Border management / border security
- Citizen ID

IRISCAM API

IrisCam API is a software library included in the SDK that provides abstraction of several market leading iris cameras. Support for new cameras is added in subsequent revisions of the SDK as they become available. It enables the same enrollment application to be used with the different cameras over time and across the system. An up-to-date list of iris cameras supported by IrisCam API is available upon request.

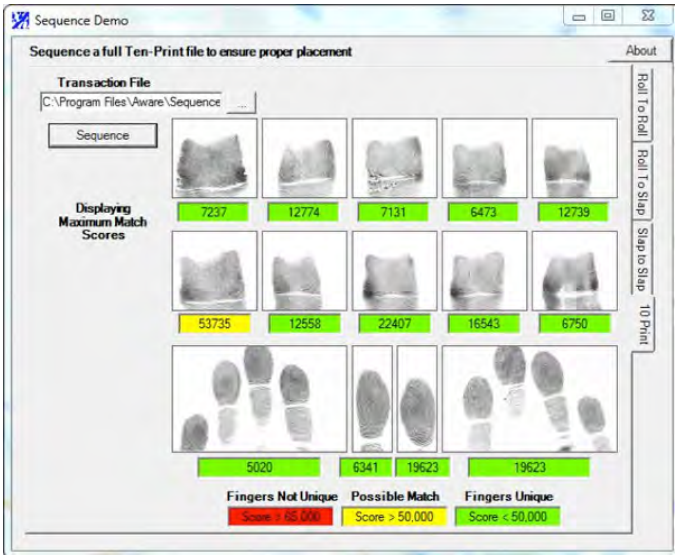
SDK FEATURES

- **Fully featured C Language API**
- **C#/.NET wrappers**
- **Example programs with source**
- **Java Native Interface support**
- **Microsoft Windows and Linux support**

SequenceCheck™

Fingerprint segmentation, sequence checking, and quality scoring for advanced quality and compliance assurance

SequenceCheck provides matching and image quality measurement for multi-finger live scan and card scan systems. It is an API designed for applications requiring a high level of fingerprint image quality assurance. The collection of fingerprint image data for government, civil applicant, immigration, or criminal databases typically includes the collection of two sets of four-finger "slap" images, ten rolled finger images, and an "impression" of each thumb. Errors can occur during the acquisition of fingerprint image data during the live scan or inking process. For example, the impressions can be placed in the roll locations, or the roll images can be arbitrarily placed into the wrong boxes on the paper or electronic record. The images can be smudged or of low contrast. SequenceCheck is broadly used, highly accurate, and error-resilient.



SequenceCheck reports match scores between slaps and rolls of each finger.

SequenceCheck helps to maintain the integrity of the image data, and improve biometric matching performance by confirming that each finger meets a minimum image quality threshold, and that it is properly identified.

SequenceCheck applies several advanced algorithms to perform the following tasks:

SLAP SEGMENTATION

This is the process of partitioning each multi-finger image into multiple single finger images. These images can consist of a four-finger "slap" or any combination of one to four fingers.

SINGLE FINGER SEGMENTATION

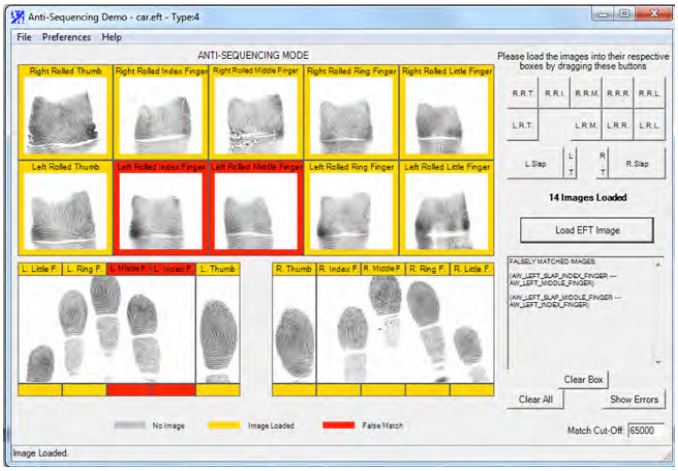
This is the process of extracting only the single contiguous fingerprint image data from a larger image. This process removes noise and dirt from the periphery of the image and centers the finger print image data in a new, clean image.

FINGERPRINT IMAGE QUALITY SCORING

This step involves the generation of statistics and measurements on the fingerprint image data using QualityCheck. The raw data can be returned so a quality score can be tuned to meet the characteristics of the scanning device, or a single image quality score can be returned based on a combination of the measurement data. Image quality scores reflect contrast, brightness, image size, ridge flow, and minutiae counts.

FINGERPRINT ENCODING

This is the process by which the minutiae data and the core/delta regions of each image are determined. This data is used in the matching process and is output to an application through an API call.



SequenceCheck reports non-matching slaps and rolls of the same finger.

FINGERPRINT IDENTIFICATION

This is the final step in the sequence; it uses the data generated by the other steps and applies a matching algorithm to the minutiae points. A match score is generated. Match/no-match can be determined by setting a threshold value. Typically, matches generate scores that are significantly higher than non-matches. In most cases, non-matches generate a score of zero.

The major function areas described above are provided through an easy-to-understand and easy-to-implement API. SequenceCheck includes example programs with source code that demonstrate how best to integrate it into a larger application. The design of SequenceCheck assumes no predefined workflow; individual functions can be called in almost any order to perform any sub-component of the sequence checking.

PALM IMAGE QUALITY CHECK

SequenceCheck provides support for palm image quality. Functionality includes leftness and rightness measurement, full hand segmentation (separation of four fingers from the full hand), comparison of upper palm with lower palm to ensure each originated from the same hand, and global quality scoring on the palm image data.

FEATURES & FUNCTIONALITY

- Optimized for speed
- ActiveX control for Visual Basic or other Visual programming environments
- Includes working demonstrations with source code
- Includes functionally separate libraries or DLLs to provide segmentation, encoding, matching and image quality measurement
- Programmable match/no-match thresholds
- Provides compliance with a system requirement for most forensic quality fingerprint systems
- Helps to minimize the likelihood of acquiring invalid or poor quality data
- Helps to maximize the likelihood of AFIS matches
- A true COTS solution designed to manage a complicated image processing task

SDK FEATURES

- Fully featured C Language API
- C#/.NET wrappers
- Example programs with source
- Java Native Interface support
- Microsoft Windows and Linux Support

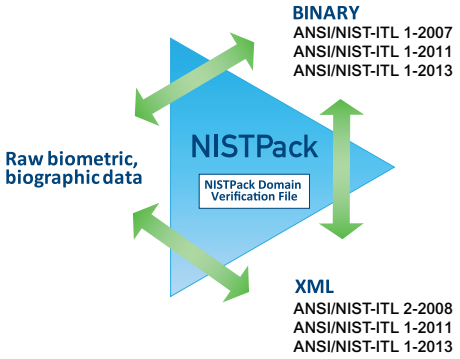
USE WITH OTHER AWARE SOFTWARE PRODUCTS

SequenceCheck can be used seamlessly with several other software products from Aware. It can be used with AccuScan to perform quality assurance on images scanned from fingerprint cards. NISTPack can be added to perform FBI-certified WSQ compression and ANSI/NIST-ITL 2013 (and earlier) compliant data formatting.

NISTPack

Read, write, edit, and validate biometric transactions in compliance with ANSI/NIST-ITL standards and derived specifications

NISTPack™ is an SDK that enables an application with reading, writing, viewing, editing, and validating of biometric data transactions in compliance with ANSI/NIST-ITL 1-2000, -2007, -2011 and 2-2008 standards. Using NISTPack ensures that biometric images are properly compressed, demographic data is included in the correct format, and the resulting object is constructed properly for data interchange between standards-based biometric systems.



NISTPack provides a common C# or Java API to create and validate biometric transactions that comply with either the traditional binary encoding of the standard or the XML encoding of the standard. Raw biometric image and biographic data can be input and the API design facilitates the output of either format. The same API functions are used to create either format.

Additionally, NISTPack supports the two-way conversion between binary encoded data and XML encoded data in compliance with the standard.

READ, WRITE, EDIT AND VALIDATE FUNCTIONALITY:

Reading information from a transaction file. This entails reading the file into an internal format and providing access to the transaction's image and textual data. This might be done by users who need to display the information contained in a transaction file.

Creating a transaction file. This entails building up a transaction from image and text information into a valid transaction file. This might be done by users who need to generate submissions of ten-print files or for any other type of transaction.

FEATURES & FUNCTIONALITY

- Includes FBI-certified, high-performance WSQ fingerprint image compression
- Simple image insertion and extraction with automatic compression/decompression as specified by the standard for each record type
- JPEG 2000 support for 1000 ppi finger and palm images in compliance with the profile required by the standard "Profile for 1000 ppi Fingerprint Data"
- JPEG and JPEG 2000 support for Type-10 records
- Lossless JPEG 2000 and PNG support for Type-13 records
- Lossy/lossless JPEG 2000 and lossless PNG for Type-17 records
- Predefined verification files for over 20 domain implementations in simplified format that serves as a baseline for additional individual domains
- Supports all record types of the standard (including fingers, palms, faces, irises, latents, minutiae, scars/marks/tattoos, and CBEFF objects)
- Two way conversion between the binary (ASCII separated) and XML (NIEM compliant) versions of the standard
- Enhanced JavaScript-based validation engine used to generate custom error checking and validation

Editing of transaction files. This entails making changes to existing files or correcting items and assuring that the new file is compliant.

Verification of a transaction file. This entails examination of the transaction file for compliance with the general transaction format given by the ANSI/NIST specification or by a more specific implementation like the FBI's EFTS specification or a state specific implementation. The user could determine if the transaction is compliant or if it is not, generate a detailed list of errors.

SDK FEATURES

- APIs to develop applications to read, write, edit and view ANSI/NIST-compliant biometric data
- Run-time applications and demos with source code
- Single API to create both types of structured data (binary and XML)
- C++, .NET, and JNI versions available
- Pure Java version available as JNISTPack
- Fully featured C Language API
- C#/.NET wrappers
- Example programs with source
- Support for
  - Java Native Interface
  - Microsoft Windows
  - Linux
  - Sun Solaris
  - HP-UX
  - IBM AIX
  - Apple iOS and Android (NISTPack Mobile)

RECORDS SUPPORTED

ANSI/NIST-ITL standards are widely used globally and support several different types of biometric and demographic data. NISTPack provides API support to insert and remove any full record, field, subfield, or item from an interchange file. NISTPack provides an easy-to-use library of functions that simplify the process of ANSI/NIST-ITL compliant formatting of the following into a single compact record defined by ANSI/NIST-ITL:

- biographic data (Type-1 and 2 records)
- WSQ compressed fingerprint image data (Type-4 record)
- user defined gray scale images (Type-7 record)
- digitized signature data (Type-8 record)
- minutiae data (Type-9 record)
- expanded Type-9 minutiae record that supports latent image extended feature sets (EFS)
- facial, scar/mark, and tattoo data (Type-10 Record)
- latent images (Type-13 records)
- variable resolution (500 and 1000 ppi) finger images and 4-4-2 (left, right hand and dual thumbs) (Type-14 records)
- palm images at 500 and 1000 ppi (Type-15 Record)
- test images (Type-16 Record)

Display of Type-4 records in transaction editing tool

- iris images (Type-17 Record)
- DNA record (Type-18)
- plantar (footprint image) record (Type-19)
- source representation data image record (Type-20)
- associated context image record (Type-21)
- information assurance record (Type-98)
- Other biometric data not handled by the other records (Type-99 Record)

AGENCY-SPECIFIC IMPLEMENTATIONS SUPPORTED

NISTPack supports both the generic ANSI/NIST standard and agency-specific implementations of the standard. Through a text-based rule file called the NISTPack Validation File, NISTPack supports read/write and validation of most of the global agency-specific implementations (domains) of the standard defined. This includes:

- FBI EBTS, all versions including the XML version
- US DoD (all versions)
- EU BMS
- Interpol
- RCMP (all versions)
- Five Country Consortium (FCC)
- UK Home Office
- German Federal Police (BKA)
- New Zealand Police
- Western Identification Network (WIN)
- Most US States

ICAOPack™

Data reading, personalization, and authentication for e-passport solutions in accordance with ICAO Doc 9303

ICAOPack™ is an SDK that provides conformance with ICAO LDS and authentication standards specified in ICAO Doc 9303 Part 1 Volume 2 e-passport standards as well as associated ISO/IEC 19794 biometrics standards.

ICAOPack is a flexible API and utility set designed to read, write, validate, and view standards-compliant biometric image and template data. ICAOPack ensures that data generated for storage can be read by other systems, or similarly, that a system can read the data from any standards-compliant passport.

ICAOPack's Smart Card Library utilizes the PC/SC interface for reading the contactless e-passport chip. ICAOPack's Security Library provides comprehensive support for Extended Access Control (EAC), Basic Access Control (BAC), Passive Authentication, and Active Authentication.

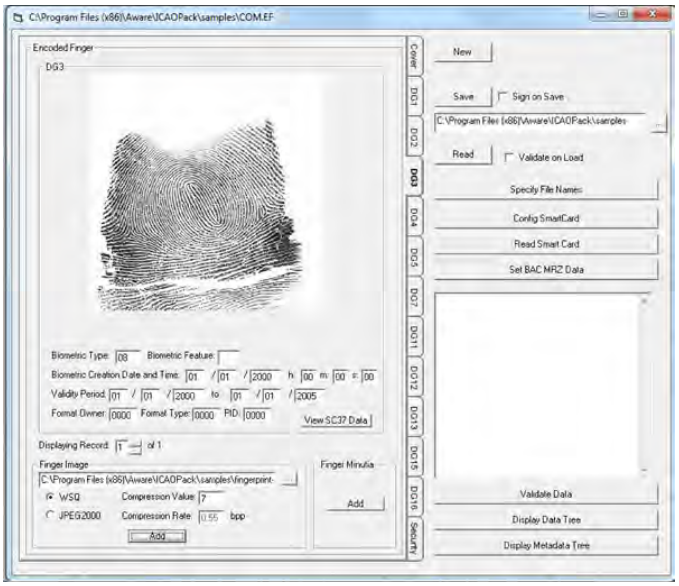
ICAOPack includes JPEG 2000, JPEG, and WSQ compression and decompression of biometric images, as well as quality scoring for fingerprint images. This advanced algorithm generates a score for a fingerprint image to help operators use only fingerprint images of sufficient quality for biometric matching.

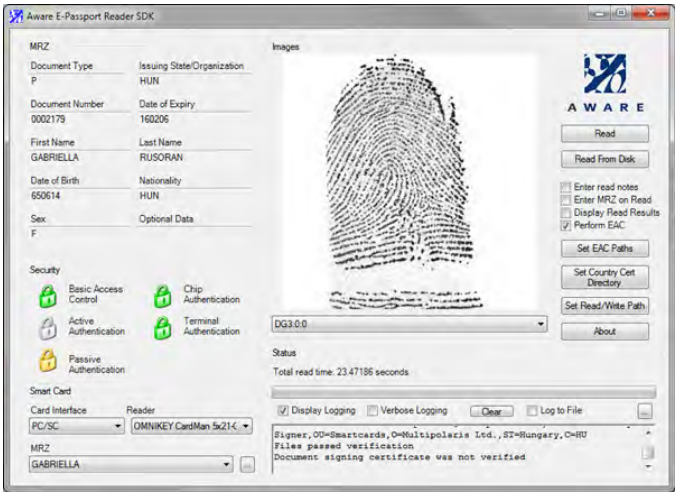
APPLICATIONS

- E-passport personalization and issuance
- Citizen ID
- Border management

FEATURES AND FUNCTIONALITY

- Supports multiple facial, finger images, finger minutiae, and iris data sets
- Provides CBEFF, ISO/IEC 19794, ICAO LDS file packing, unpacking, and reformatting
- CBEFF, ISO/IEC 19794, ICAO LDS file content verification
- Supports extended access control, basic access control, active authentication, and passive authentication
- Ensures file structure and integrity
- Utilizes PC/SC for contactless e-passport chip reading
- Includes WSQ, JPEG 2000, and JPEG compression
- Includes Aware QualityCheck API





SDK FEATURES

- Easy to use and understand
- Fully featured C Language API
- C#/.NET wrappers
- Programmable in C, C++, .NET, and Java
- Example programs with source
- Java Native Interface support
- Microsoft Windows and Linux Support
- Android and iOS support (ICAOPack Mobile)

PIVPack™

FIPS 201-compliant PIV card reading, personalization, and middleware

PIVPack™ is an SDK that enables a software application with formatting, validating, and parsing of biometric, biographic, and security object data in compliance with FIPS 201 and companion documents SP 800-76 and SP 800-73. PIVPack includes Security Library and also Smart Card Library, a NIST-certified PIV Middleware API.

PIVPack can be used to incorporate data formatting and security functionality into PIV registration, personalization, and card reader applications. PIVPack can also be used to create equivalent XML files, such as for registration data transport.

PIVPack is certified by US GSA as compliant with the product category of PIV Middleware. It is listed on the GSA Approved Products List (APL).

BIOMETRIC DATA FORMATTING

PIVPack enables designers to build compliant data formatting and parsing into system workflow through a simple API. All data formatting, reading, and writing performed by PIVPack is managed by XML-based configuration files that describe the details of the data object to be created, parsed or validated. The biometric facial image may optionally be retained and/or stored on the card, in which case it must be compliant with ANSI/INCITS 385. The fingerprint images must be compliant with ANSI/INCITS 381 and retained for archival purposes. The fingerprint templates stored on the card must be compliant with ANSI/INCITS 378. Each object must be "wrapped" with a PIV Patron Format variant of CBEFF.

BIOMETRIC SECURITY LIBRARY

Several of the data containers on the PIV card must be signed. To address this requirement, PIVPack includes a supplemental library called "Biometric Security Library" which implements compliant encryption and hashing algorithms to verify the signatures and the SOd. PIVPack parses the data and accesses the certificates for use by the Biometric Security Library. Additionally, the Biometric Security Library can utilize the document signing certificates and the private keys provided by the PKI to sign the data objects.

FEATURES & FUNCTIONALITY

- Software development kit with example programs and documentation
- Provides FIPS 201-compliant file packing, unpacking and reformatting
- Conversion from proprietary formats to FIPS 201 format
- Import/export of common image formats
- File content verification
- Signing and verifying of digital signatures

APPLICATIONS

- Employee credentialing
- Access control

PIVPACK COMPONENTS

PIVPack includes several components useful for enrollment, personalization, and card reading:

- Data collection and error checking according to SP 800-73 and SP 800-76
- PIV file formatting and reading in full compliance with SP 800-73 and SP 800-76 for PIV ID card personalization
- Fingerprint minutiae extraction (optional add-on) and template creation in compliance with ANSI/INCITS 378 (MINEX certification pending)
- Security object generation and PKI authentication in compliance with SP 800-73
- Certified PIV middleware API
- PC/SC smart card interface

SDK FEATURES

- Easy to use and understand
- Programmable in C/C++, Java, VB, and .NET
- Supports CBEFF, face image and finger minutiae data sets
- Ensures file structure and integrity
- Fully featured C Language API
- C#/.NET wrappers
- Example programs with source
- Java Native Interface support
- Microsoft Windows and Linux Support
- Android and iOS support (PIVPack Mobile)

AccuScan™

FBI-certified scanning and digitization of fingerprint cards

AccuScan is an add-on module for NISTPack that together with any of several market-leading consumer-grade flatbed scanners enables an FBI-certified solution to scan and digitize paper tenprint cards. The FBI requires compliance with its EFTS IQS (Electronic Fingerprint Transmission Specification - Image Quality Specification) for fingerprint card scanning solutions.

Related products include AccuScanMB for high-volume, automated batch processing of fingerprint cards and FormScanner, an application that can be used to assist and administer the card scanning process.

Together, NISTPack and AccuScan provide a fully programmable and configurable software tool that enable systems integrators to design and deploy a tenprint card scanning system that is fully FBI compliant.

The combined NISTPack/AccuScan software toolset provide the following:

- **FBI IQS Appendix F compliance for a scanner**
- **FBI certified WSQ compression and decompression**
- **Fingerprint image quality measurement and Q/A**
- **Read, write, view, edit FBI EFTS civil applicant and criminal tenprint transactions**
- **Validate and error-check FBI EFTS submission files (electronic tenprint cards) and FBI responses (ident, no-ident, or error)**

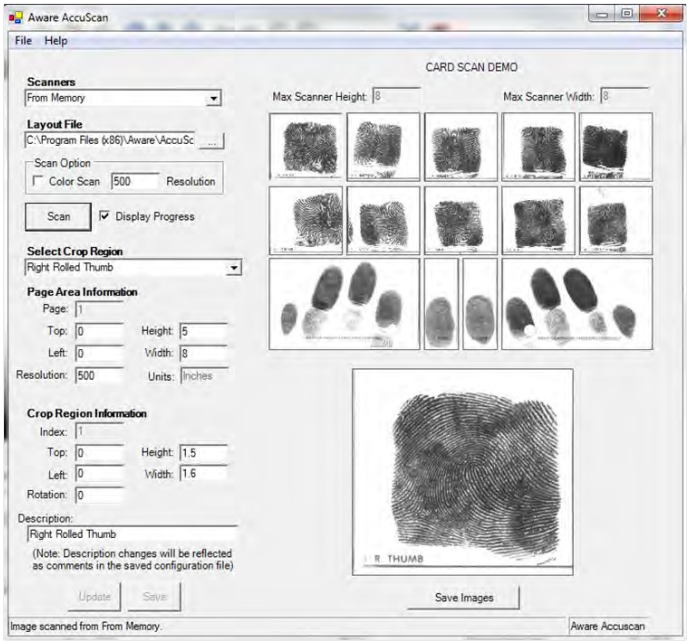
The figure to the right shows the user interface of the AccuScan reference application. The individual fingerprint images have been cut out of the larger scanned image, compressed with WSQ and inserted into the EFTS file as separate Type-4 records. The source code to this program is provided as part of the AccuScan development kit.

FEATURES & FUNCTIONALITY

- **Eliminates all work associated with FBI certification of flatbed scanners**
- **Supports commercial and consumer-grade scanners**
- **Along with NISTPack, provides a full FBI- and NIST-compliant development toolkit from inked paper cards to electronic submission and response management**
- **Greatly shortens development time of card scanning solutions**
- **Easy to maintain and customize for each agency**

APPLICATIONS

- **Fingerprint recognition**
- **Automated fingerprint identification systems (AFIS)**
- **Law enforcement**
- **Defense**
- **Border management**



AccuScan reference application

Card Template Tool

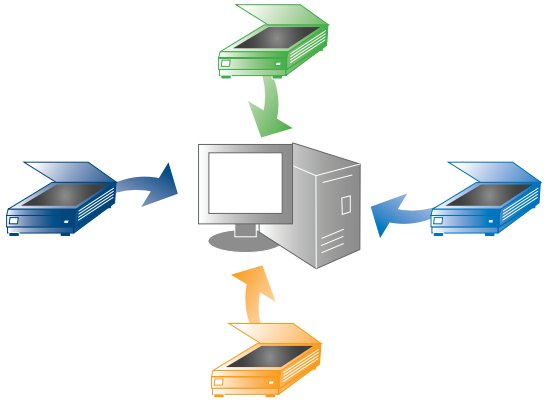
All U.S. state and federal government agencies maintain and utilize a unique set of fingerprint cards and forms. Some states have five or six different cards, and each card is used for a different purpose, depending upon the reason for obtaining the inked prints.

AccuScan manages this problem through an XML-based configuration file that holds the layout details of the original paper document. This file describes the size and location of each fingerprint or palm print image. AccuScan includes a utility (executable and source) that enables the easy creation of these XML configuration files. The process includes scanning of a blank or populated original card, loading it into the Template Tool, and then tracing the fingerprint image boxes. After all image regions of interest have been selected, the file is saved and can be used by an AccuScan runtime application.

Also see Aware's FormScanner applications for fingerprint card and form scanning.

AccuScanMB for High-Volume, Automated Batch Processing of Fingerprint Cards

AccuScanMB is an enhanced version of AccuScan designed to enable "multi-batch" fingerprint card scanning though a parallel configuration of up to six off-the-shelf flatbed scanners equipped with automatic document feeders (ADF). Each scanner can process up to 160 500 ppi cards per hour or 48 1000 ppi cards per hour. With six scanners running in parallel, nearly 1000 500-ppi cards can be processed every hour. Like AccuScan, AccuScanMB provides Appendix F-certified scanning at 500 and 1000 ppi, and maintains AccuScan's configuration, cropping functionality, and API.



AccuPrint™

FBI-certified printing of digital fingerprint records

AccuPrint is an SDK for FBI-certified printing of high-quality digitized fingerprint images using consumer-grade laser printers. AccuPrint can print a single fingerprint image, palm image, or an entire agency specific tenprint card with text and graphics. When used with certain 1200 dpi laser printers, AccuPrint is FBI-certified as compliant with Appendix F Printer Specifications. As a stand-alone library, AccuPrint accepts uncompressed fingerprint images as TIF, BMP, or raw image files. It processes each image separately and generates a new, high-quality, image suitable for printing.

ACCUPRINT WITH NISTPACK: A FULL "NIST FILE TO PRINTED CARD" SOLUTION

When AccuPrint is used with NISTPack, it provides an elegant solution that generates a printed tenprint card from the contents of an ANSI/NIST compliant transaction file or an FBI EFTS file. NISTPack parses the NIST file, WSQ decompresses the fingerprint and palm images, and JPEG decompresses mug shot or scar/mark/tattoo images.

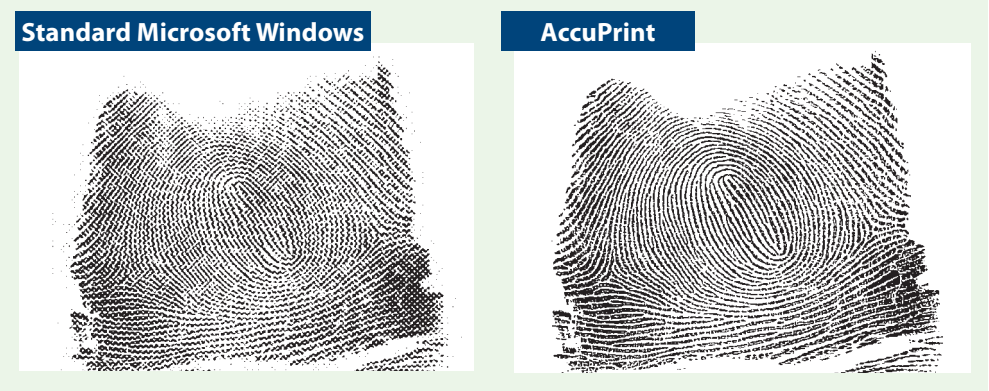
AccuPrint receives the image and text data from NISTPack and prints each fingerprint image to a specified location on an 8x8 card or to standard paper stock. It prints the card graphics and demographic data from the Type-1, Type-2, and Type-10 records into user-specified locations on the tenprint card.

APPLICATIONS

- Fingerprint recognition
- Automated fingerprint identification systems (AFIS)
- Law enforcement
- Defense
- Border management

FEATURES AND FUNCTIONALITY

- FBI-certified with several printers
- Prints to standard paper stock, blank tenprint card stock, or pre-printed tenprint cards
- Prints front and back of cards
- Prints agency specific tenprint card text and graphics
- Dramatically improves the native printing capability of Microsoft Windows or Unix
- Cost-effective solution supports off-the-shelf printers
- Meets the FBI Image Quality Specification (IQS) for printers



Quality comparison: The image on the left has been printed with the Microsoft Windows native printing process. The live scanned image on the right has been processed and printed with AccuPrint.

GENERATING TENPRINT CARD GRAPHICS

AccuPrint enables printing of agency-specific tenprint and palm print cards through two methods:

1. Text-based layout files

These files use a simple suite of line and text drawing commands to draw every line and text segment present on the card. The files also allow the use of graphical images and icons.

2. Scanned image of a blank card

A blank tenprint card scanned and saved as a TIF or JPEG image can also be used by AccuPrint to regenerate tenprint card graphics. This method is particularly useful for cards with complicated graphics, fonts, or character sets.

PRINTING OF PALM PRINT IMAGES

AccuPrint supports the printing of full palm with fingers, partial palm, and writer's palm. It supports the rotation of the palm images, which may be required to match the way in which the palm image should be placed on the card.

BARCODE PRINTING

Tenprint cards often include a barcode that was stored in the digital form of the card, typically in a Type-2 field of the NIST record. AccuPrint can generate valid barcodes that comply with the code 39 format, the code 128 format and the PDF417 (two dimensional format).

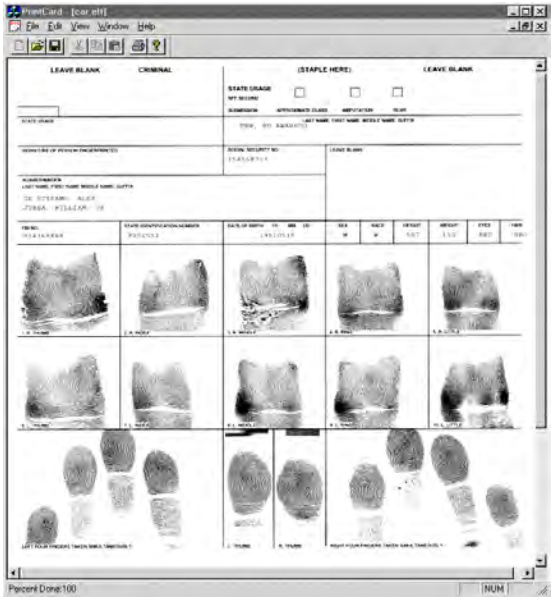
JAVASCRIPT-BASED LOGIC

The AccuPrint layout file uses JavaScript to enable a developer to add simple logic to the printing process. In some cases, the printed form of demographic text must be formatted differently than how it is stored digitally in the NIST file. Examples of this include:

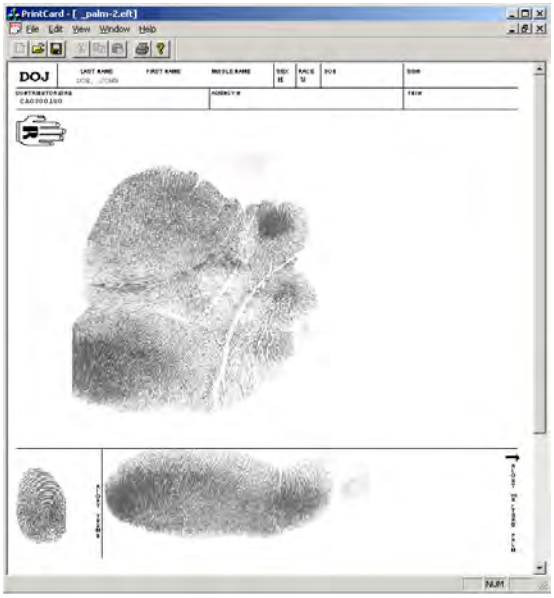
- **Dates (month, day, year) that must be rearranged**
- **Insertion of hyphens or slashes between data**
- **Check marks in checkboxes based on the contents of a demographic data field**

SDK FEATURES

- **Includes documentation and example programs for ease of use**
- **C language API for software developers**
- **ActiveX control for Visual Basic programming**
- **Includes runtime applications and demos with source code**



The print preview of the AccuPrint "PrintCard" utility showing a tenprint card. AccuPrint generates all text and graphics. Demographic data is mapped from the NIST file to the correct location on the card. The source code to this utility program is provided as part of the SDK.



The print preview of the AccuPrint "PrintCard" utility showing a palm print card. When used with NISTPack, the palm image is extracted out of the Type-15 record, decompressed, and printed by the AccuPrint engine.

AwareWSQ1000

High-performance, FBI-certified WSQ compression of fingerprint Images with JPEG 2000 compression and transcoding for 1000 ppi Images

Aware WSQ1000 is an SDK providing the industry's highest-performing, FBI-certified implementation of the WSQ compression algorithm for fingerprint images. WSQ (Wavelet Scalar Quantization) is a wavelet-based compression standard designed and specified by the FBI for compression of high-resolution, 500 ppi grayscale fingerprint images. Aware WSQ1000 includes JPEG 2000 compression for 1000 ppi images and efficient transcoding between WSQ and JPEG 2000.

Aware WSQ1000 was the first commercial implementation of the gray scale fingerprint image compression standard. Its origins date back to 1994-1995 when Aware participated in a standards forum with US government agencies and several US universities to develop a lossy compression algorithm specifically for gray scale fingerprint data. A wavelet-based technique known as Wavelet Scalar Quantization (WSQ) was adopted.

Today, most of the world's large, high throughput, fingerprint management and matching systems depend on Aware WSQ1000 to manage the compression and decompression of finger and palm image data. All finger and palm images submitted to the FBI are managed by Aware WSQ1000.

- **Runtime performance.** Aware WSQ1000 is 4-5 times faster than most other WSQ implementations that share a common code base
- **Error resilience.** Aware WSQ1000 has been exposed to and processed more images than any other implementation of the standard. It will not crash or bring a system down when presented with a non-compliant, truncated, very large, or unusually formatted image.
- **Dedicated support and maintenance.** Aware WSQ1000 is a high quality commercial implementation designed and maintained by professional software engineers explicitly for demanding production environments

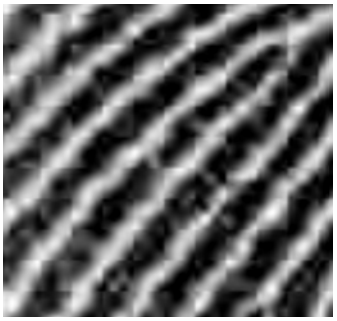
FEATURES & FUNCTIONALITY

- Fast, reliable compression and decompression of critical fingerprint image data
- Technology developed, maintained, and fully supported by Aware
- Complete, fully-featured API facilitates efficiency and ease of use
- Efficient transcoding from 1000 ppi JPEG 2000 images to 500 ppi WSQ images
- Support for all necessary JPEG 2000 compression options and comment insertion into the JPEG 2000 or WSQ codestreams
- Precise rate control, enabling compression to within 1% of specified ratio, file size, or bit rate (bits/pixel)

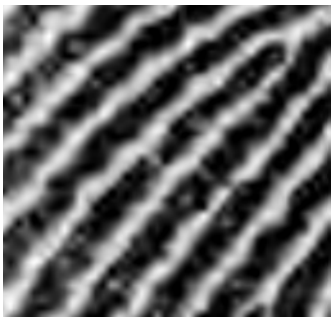
SDK FEATURES

- Fully featured C Language API
- C#/.NET wrappers
- Example programs with source
- Java Native Interface support
- Support for
  - Microsoft Windows
  - Linux Support
  - Sun Solaris
  - HP-UX
  - IBM AIX
  - Java
  - Apple iOS and Android (WSQ Mobile)

- **Continuous FBI compliance certification.** All finger and palm images compressed with Aware WSQ1000 contain an encoder ID assigned by the FBI which is specific to the operating system and revision of the software. Compliance testing and certification is important because the purpose of the standard is to ensure minimal data loss of friction ridge detail. The WSQ standard is of minimal value without compliance assurance.

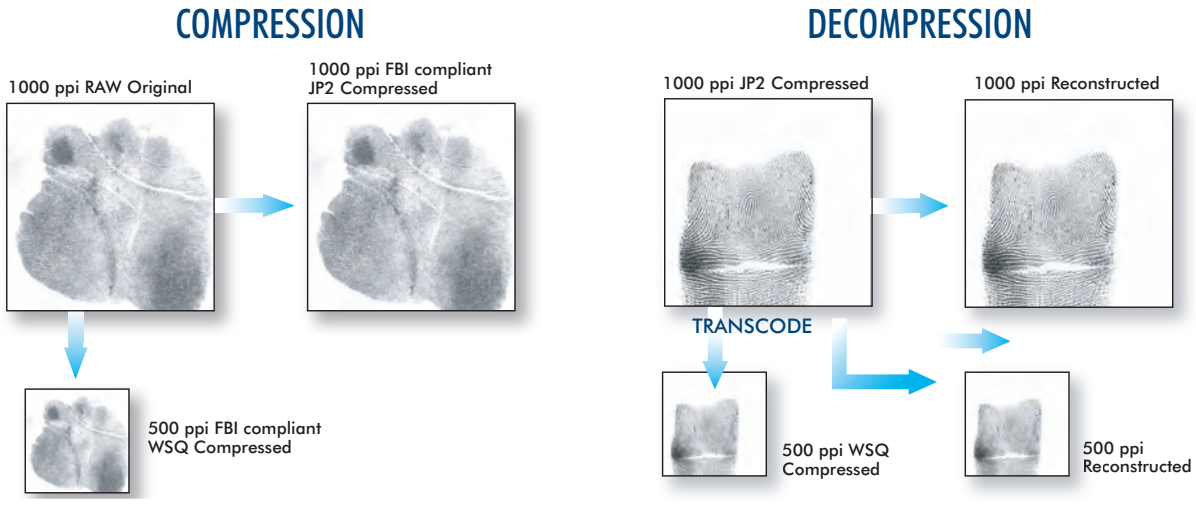


Section of a digital fingerprint image that has been compressed 15:1 with the JPEG algorithm. Note the block artifact that is inherent in the algorithm. The image has been zoomed by 4.



Section of the same fingerprint image that has been compressed 15:1 with the WSQ algorithm. Note the absence of the block artifact. The image has been zoomed by 4

- **Support for 1000 ppi images.** The FBI has published a standard for the compression and formatting of 1000 ppi fingerprint and palm images, called "Profile for 1000 ppi Fingerprint Compression." This standard requires the use of JPEG 2000 for compression and formatting of 1000 ppi fingerprint images. WSQ will continue to be used for 500 ppi images. Like WSQ, JPEG 2000 uses a wavelet-based compression algorithm that performs particularly well for large images. It is an established ISO/IEC standard used extensively for applications involving large images including medical imaging, digital archiving, and digital cinema. The JPEG 2000 standards are complex, with many variable settings intended to help optimize its use for different applications. The FBI 1000 ppi profile includes several mandatory encoding parameters to ensure the optimization of JPEG 2000 for fingerprints. The FBI's IAFIS and most legacy AFIS systems will continue to require 500 ppi WSQ compressed data. In order to enable 1000 ppi fingerprints to be used in both 1000 ppi and 500 ppi systems, Aware WSQ1000 enables efficient transcoding from 1000 ppi JPEG 2000 images to 500 ppi WSQ images.



Fingerprint and palm images can be compressed, decompressed, and transcoded between WSQ and JP2.

Aware JPEG 2000

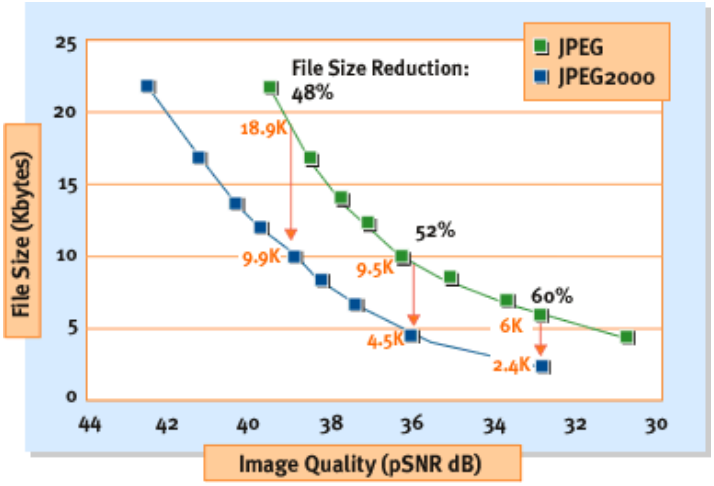
For compression and decompression of biometric face and iris images

JPEG 2000 is an international image compression standard (ISO/IEC 15444) referenced--and in some cases recommended--by biometrics standards for face and iris image compression. Several published technical reports cite the superior performance of JPEG 2000 as compared to JPEG. JPEG 2000 is used extensively for applications involving large images including medical imaging, historical archiving, and digital cinema. JPEG 2000 is also used for compression of 1000 ppi fingerprint images (see Aware WSQ1000).

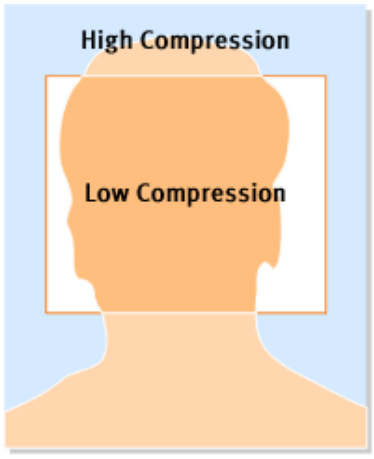
Aware's JPEG 2000 compression libraries are available as a standalone SDK or as part of several other Aware SDK products.

KEY JPEG 2000 FEATURES FOR BIOMETRIC IMAGE COMPRESSION

- Up to 50% smaller image files than JPEGs of the same image quality
- Accurate file size targeting
- Accurate image quality targeting
- Performs beyond compression ratios where JPEG breaks down, enabling compression of high-resolution images
- Multiple images and formats can be extracted from a single JPEG 2000 image file: lossy or lossless, color or grayscale, thumbnails, etc.
- Region of Interest encoding allows different compression ratios for different areas of the image
- Advanced error resiliency features prevent file damage during transmission in noisy environments



File size reduction of a facial image



Region of Interest

FIDOSuite™

FIDO® Certified SDKs for mobile biometric authentication

Aware's FIDO® Suite is a family of SDKs for mobile biometric authentication that are certified conformant with the specifications of the FIDO Alliance and interoperable with other FIDO-certified products. Aware's Face and Face+Voice Authenticators are UAF v1.1 Level 1 FIDO® Certified.

ABOUT FIDO

FIDO specifications aim to define frameworks for authentication online from PCs and mobile devices. There are two sets of FIDO specifications: UAF (Universal Authentication Framework) for password-free authentication, and U2F (Universal 2nd Factor) for second-factor authentication. Aware's FIDO® Suite products are certified compliant with the FIDO specifications for UAF. They include three categories of products: FIDO Server, FIDO Client, and FIDO Authenticators.

UAF enables a user to login to a website using biometrics or other means instead of a password. FIDO specifications ensure that private identity information including biometrics is always captured, verified and retained on the user's device and never sent remotely up to a server. FIDO also offers plugability, by modularizing the architectural into various components, each with standardized interfaces that facilitate interoperability.

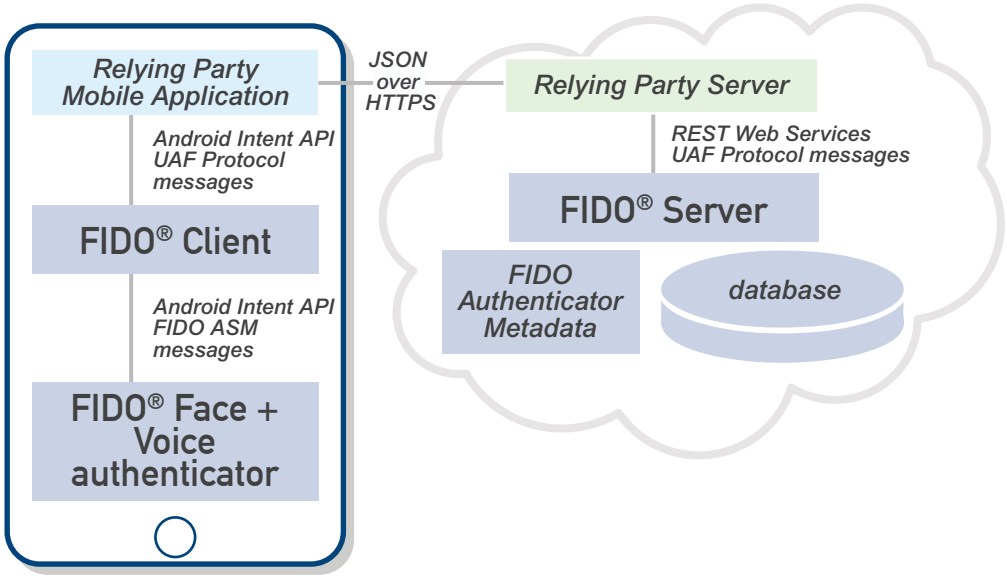
HOW IT WORKS – REGISTRATION

FIDO authentication employs a challenge/response mechanism using digital signatures. A user must first access a specific app or website and complete a registration process before using FIDO. The user submits their biometrics and PIN during this registration.

For every successful biometric/PIN match during registration, a public key pair is created. The private key is retained on the client in a cryptographic keystore, and the public key is sent to the server, where it is saved in a keystore under the user's ID.

HOW IT WORKS - LOGIN

Upon a login attempt, the FIDO Authentication Server creates a random challenge and sends it to the FIDO Client. The biometrics and PIN are matched locally by the FIDO Authenticator against the biometrics enrolled for that user; they are never transmitted to the server. The user is prompted again to enter his biometrics/PIN. If the match attempt is successful, it unlocks the private key from the FIDO Client keystore. The FIDO Client signs the challenge using the user's private key and sends it to the FIDO Server. The server verifies the signature using the public key received during registration, and the user is permitted to login.



FIDO Authenticators

FIDO® FACE AUTHENTICATOR

Aware' FIDO Face Authenticator uses facial recognition for biometric authentication, with a user interface that enables a user to capture his/her face and robust active and passive liveness detection techniques to prevent spoofing. The captured face and voice data is stored in a template form, and is used for subsequent login to FIDO-enabled servers.

FIDO® FACE+VOICE AUTHENTICATOR

Aware's FIDO Face+Voice Authenticator uses both face and voice recognition and liveness detection for biometric authentication. It captures face and voice simultaneously during authentication, applying active and passive face and voice-based liveness detection methods to prevent spoofing attacks.

FEATURES AND FUNCTIONALITY

- **Mobile face and voice recognition for biometric authentication**
- **Performs autocapture and quality assessment of the user's biometrics**
- **Performs matching of the user's facial biometrics**
- **Performs active and passive facial liveness detection**
- **Maintains users' public/private key pairs in a cryptographic keystore for each relying party**
- **Abstracts the device camera**
- **UAF version 1.1 Level 1 FIDO® Certified**

FIDO Client

Aware's FIDO® Client is the intermediary application that helps to bind FIDO authenticators with the relying party mobile application. A FIDO client can look up all FIDO authenticators on the device, and communicate via JSON messages standardized by the FIDO ASM API. Similarly, a relying party mobile application can look up a FIDO client and communicate with FIDO Client. The messages between a relying party application and FIDO Client are standardized via FIDO UAF Protocol Specification and FIDO UAF Application API specification.

FIDO Client can create an UAF Protocol payload, embed it as part of a larger message, and transmit it via the Android intent mechanism to the mobile application layer. The application could embed this message as part of its payload to the relying party server, which then communicates with a FIDO server.

FIDO Client serves as the glue that can link any relying party mobile application that requires the FIDO functionality with the different FIDO authenticators on the device, possibly provided by different vendors.

FEATURES AND FUNCTIONALITY

- **Performs communication with a FIDO server using the UAF standard API (JSON objects over HTTP)**
- **Performs communication with the various authenticators using the UAF authenticator abstraction API**
- **Is pluggable into a web browser or a mobile application**
- **FIDO® Certified**

FIDO Server

Aware's FIDO® Server enables a relying party server to offer FIDO-based login from their mobile applications. FIDO® Server encapsulates the FIDO features required at the server, such as maintenance of the FIDO login policies, management of the public keys, and verification of the signatures created on the mobile device. It exposes REST-style web services that can be consumed by a relying party server to enable FIDO functionality.

The messages consumed or generated by the FIDO Server are also governed by the FIDO UAF Protocol Specification. A relying party server and mobile applications act as carriers of the UAF protocol messages.

FEATURES AND FUNCTIONALITY

- **registration service**
- **login service**
- **deregistration service**
- **FIDO® Certified**

Mobile SDKs

Nexa|Face™ Mobile

FACIAL RECOGNITION AND AUTHENTICATION ON A MOBILE DEVICE

Nexa|Face Mobile is an implementation of Aware's Nexa|Face facial recognition algorithm optimized for mobile devices and ported to Android and iOS. It features the strong matching performance and intuitive, easy-to-use API of Nexa|Face but is designed for operation on devices with lower memory and processing power than a PC. Nexa|Face works seamlessly with PreFace Mobile, which performs facial image autocapture, liveness detection, and compliance assurance to improve matching reliability and capture success. Nexa|Face is ideal for mobile authentication applications and is also available in Aware's FIDO UAF Face Authenticator.

Nexa|Fingerprint™ Mobile

FINGERPRINT RECOGNITION AND AUTHENTICATION ON A MOBILE DEVICE

Nexa|Fingerprint Mobile is an implementation of Aware's Nexa|Fingerprint matching algorithm optimized for mobile devices and ported to Android and iOS. It features the strong matching performance and intuitive, easy-to-use API of Nexa|Fingerprint but is designed for operation on devices with lower memory and processing power than a PC. Nexa|Fingerprint works seamlessly with Aware's other mobile fingerprint SDKs including LiveScan API Mobile, NISTPack Mobile, and Aware WSQ1000 Mobile.

Nexa|Voice™ Mobile

Nexa|Voice Mobile is an implementation of Aware's Nexa|Voice speaker recognition algorithm used for voice authentication, optimized for mobile devices and ported to Android and iOS. It features the strong matching performance and intuitive, easy-to-use API of Nexa|Voice but is designed for operation on devices with lower memory and processing power than a PC. Nexa|Voice includes features for ease-of-capture and liveness detection. Nexa|Voice is included in Aware's Knomi biometric authentication framework and in Aware's FIDO® Certified UAF Face+Voice Authenticators.

PreFace™ Mobile

BIOMETRIC FACIAL IMAGE AUTOCAPTURE, LIVENESS DETECTION / SPOOF DETECTION, AND QUALITY/COMPLIANCE ASSURANCE ON MOBILE DEVICES

PreFace Mobile is an implementation of PreFace optimized for mobile applications running on Android, and iOS smartphones and tablets. PreFace Mobile performs automated face finding and facial image capture using the smartphone camera, and like PreFace, performs automatic "tilt, scale, and crop" processing to optimize the image and analysis to assess the quality and standards-compliance.

PreFace Mobile includes advanced liveness detection / spoof detection to help prevent spoofing in authentication and other unattended enrollment applications. PreFace's liveness detection capabilities include an active mode that allows the user to interact with the application to demonstrate liveness such as by blinking or moving the head. It also has a passive mode that detects liveness and spoof attempts without the knowledge or participation of the user.

LiveScan API Mobile

FINGERPRINT AUTOCAPTURE AND QUALITY ASSURANCE ON MOBILE DEVICES

LiveScan API Mobile is an SDK that provides fingerprint capture device abstraction though a common API. It is ideal for applications where multiple high-quality, standards-compliant fingerprints must be collected within strict time constraints using a smartphone, tablet, or integrated capture device.

Real-time image analysis and capture logic

LiveScan API Mobile enables a biometric enrollment application with automated fingerprint capture and quality assurance. It performs real-time quality checks on finger images to ensure compliance and maximum quality before a final image is taken, dramatically improving overall capture speed. Real-time analysis of the preview mode data greatly reduces the likelihood that the captured image must be recaptured because it fails post capture quality analysis. By setting programmable quality targets

and thresholds, each fingerprint image is captured automatically only when it satisfies the above requirements.

Use with other products

LiveScan API Mobile output, along with biographical data, can be forwarded to NISTPack Mobile running on the same device to create FBI- and/or NIST-compliant Type-14 EFTS fingerprint records, acceptable for civil background check submissions.

APPLICATIONS

- **Fingerprint recognition**
- **Fingerprint authentication**

NISTPack Mobile

READING AND WRITING OF STANDARDS-COMPLIANT ANSI/NIST TRANSACTIONS ON MOBILE DEVICES

NISTPack Mobile is an implementation of NISTPack optimized for mobile applications running on Android and iOS operating systems. Like NISTPack, NISTPack Mobile includes FBI-compliant WSQ compression for fingerprints images and JPEG 2000 compression for facial and iris images; both are performance-optimized for mobile operating systems. Also like NISTPack, it enables creating, editing and writing of image and text data files compliant with ANSI/NIST-ITL 2013 (and earlier).

APPLICATIONS

- **Fingerprint recognition**
- **Fingerprint authentication**

Aware WSQ1000 Mobile

FBI-CERTIFIED FINGERPRINT IMAGE COMPRESSION AND DECOMPRESSION ON MOBILE DEVICES

Aware WSQ1000 Mobile is an implementation of Aware WSQ1000 designed and optimized to operate on mobile devices running Android and iOS operating systems. Aware WSQ1000 Mobile provides high-performance, FBI-certified implementation of the WSQ compression algorithm for fingerprint images on mobile devices.

APPLICATIONS

- **Fingerprint recognition**
- **Fingerprint authentication**

AwareXM™ Mobile

MINEX-CERTIFIED FINGERPRINT TEMPLATE EXTRACTION AND MATCHING ON MOBILE DEVICES

AwareXM Mobile is an SDK with C libraries and reference applications for performing MINEX-certified, INCITS 378-compliant fingerprint minutiae extraction, template generation, and 1:1 matching on mobile devices running Android, iOS, and Windows Phone operating systems. Fingerprint templates generated on a mobile device using AwareXM Mobile can either be matched on-device or alternatively transmitted to a server-based application such as BioSP for verification against a central template database.

AwareXM Mobile works seamlessly with other Aware SDKs optimized for mobile platforms, including PIVPack Mobile and ICAOPack Mobile. Together with these products, AwareXM Mobile can be used to generate and match fingerprint templates for on-device match-to-card for authentication to a biometric-enabled credential such as a PIV card or e-passport.

APPLICATIONS

- **Fingerprint recognition**
- **Fingerprint authentication**