AWARE

PRODUCT GUIDE

BIOMETRICS SOFTWARE

SDKs, Controls, and Applets for Enrollment

Applications for Enrollment and Analysis

Biometric Search and Match SDKs

Text Search and Identity Analytics SDKs

Middleware/Workflow Server

Cluster Computing Platform

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

TABLE OF CONTENTS

APPLICATIONS

SOFTWARE COMPONENTS

MIDDLEWARE/WORKFLOW SERVER

CLUSTER COMPUTING PLATFORM

SOFTWARE DEVELOPMENT KITS (SDKS)

Biometric Search and Match

Hardware Abstraction, Autocapture, Quality Assurance

Data Formatting & Validation

Biometric Image Compression

Fingerprint Cards

Smart Phones and Tablets

Application Specific Bundles

Text Search and Identity Analytics SDKs

For more information, please contact Aware.

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

http://www.aware.com

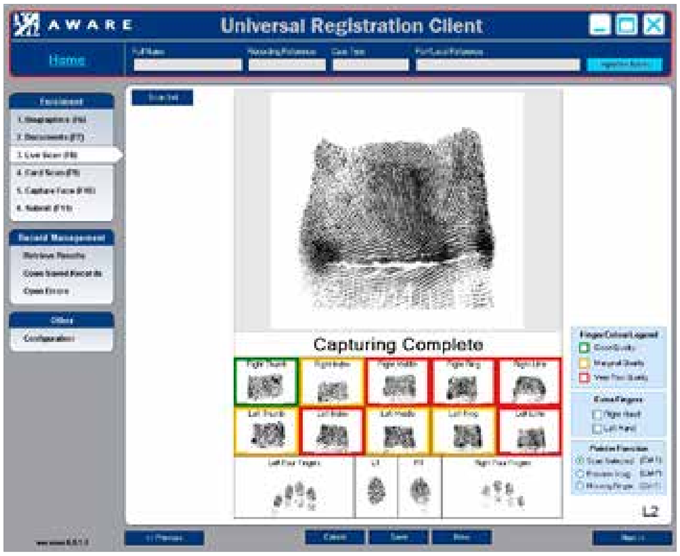
This document is for information purposes only and is subject to change without notice. Aware, Inc. assumes no responsibility for the accuracy of the information. AWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT. “Aware” is a registered trademark of Aware, Inc. Other company and brand, product and service names are trademarks, service marks, registered trademarks or registered service marks of their respective holders.

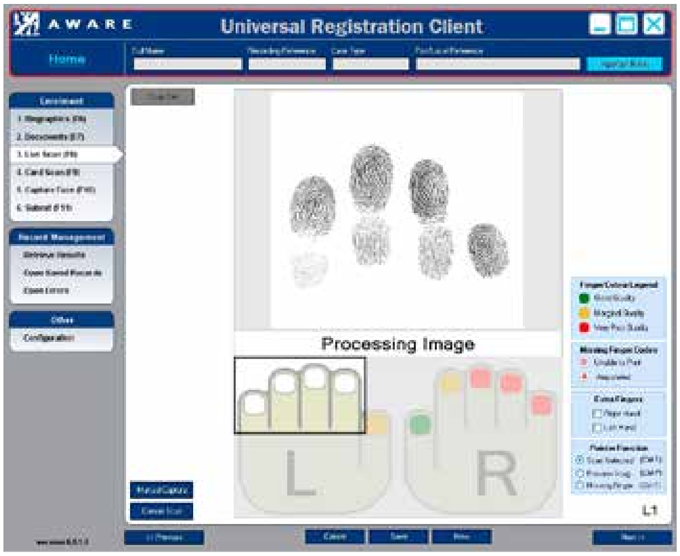
BM_product_guide_1015

Universal Registration Client (URC™)

Software Application for Biometric Enrollment

Universal Registration Client (URC) is a configurable Windows-based .NET application that utilizes Bio-Components™ and/or libraries included in Aware SDKs to perform a variety of biometric data capture, analysis, matching, formatting, and hardware abstraction functions. Customers may use URC to either quickly learn how to best implement APIs of underlying Aware software libraries, or alternatively as a baseline to develop an application customized for their own requirements and workflow.





FEATURES AND FUNCTIONALITY

- Biographic data capture, formatting, and validation
  - ANSI/NIST-ITL 1-2011 and earlier
  - ICAO Doc 9303
  - FIPS 201 SP800-76
- Tenprint autocapture
- Fingerprint matchability testing
- Fingerprint segmentation and sequence checking
- Fingerprint quality scoring
  - Aware Quality
  - NFIQ
- Fingerprint card scanning and printing
- Facial image autocapture
- Iris capture and quality scoring
- Signature capture
- Travel document scanning and authentication
- Credential personalization
  - ICAO compliant e-passport
  - FIPS 201 compliant PIV card
- Digital certificate verification
- Biometric duplicate checking
- Fingerprint template extraction and 1:1 matching for biometric authentication
- Web service-based connectivity to BioSP

URC Mobile™

Software Application for Biometric Enrollment on Military-Grade Mobile Devices

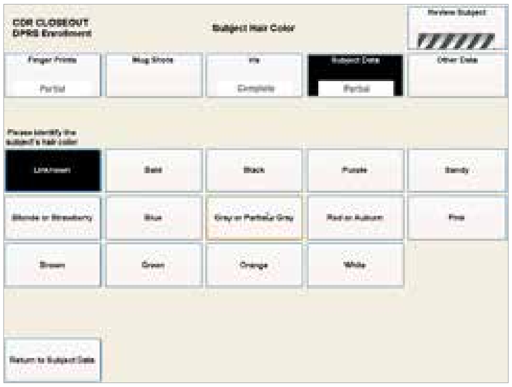
URC Mobile is a software application for performing biometric enrollment, identification, and screening on ruggedized mobile biometric devices, such as those used by military personnel in the field. It allows the operator to capture both biographic and biometric data from subjects and then match the biometric information to onboard watch lists and known mission-encountered individuals.

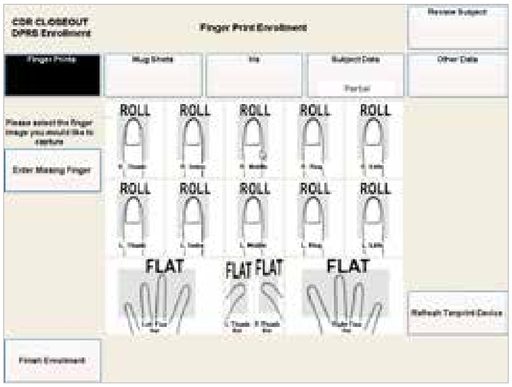
During enrollment, the operator can select the type of individual to enroll (rapid search, criminal, miscellaneous) and then collect that individual's mandatory and optional demographics, fingerprint images, facial images, iris images, document images, and cell phone information. After collection, the software performs biometric matching on the enrolled iris and fingerprint images. The application supports the uploading of watch lists in the form of EBTS files. Additionally, the application provides the ability to screen subjects (identification without enrollment). Finally, the application allows an administrator to configure the application to control the overall performance and workflow.

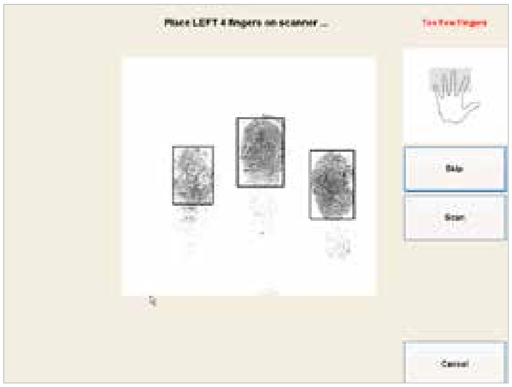
URC Mobile runs on Windows and utilizes several Aware SDKs for biometric autocapture, image quality assurance, and capture device abstraction. It supports use of many different biometric capture peripheral scanners and cameras, and operates on several COTS mobile hardware devices.

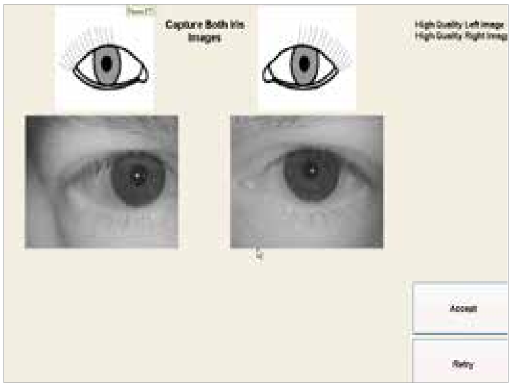
FEATURES & FUNCTIONALITY

- Support for fingerprint, face, and iris enrollment
- Collection of textual data, document images, and cell phone data
- Biometric fingerprint and iris matching
- EBTS-based watch list import
- Operation on several different COTS mobile hardware platforms
- Abstraction of peripheral capture hardware devices
- Configurable functionality and workflow









FormScanner™

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-16 records. They each utilize Aware's AccuScan, NISTPack, and SequenceCheck SDKs

Functionality Summary

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.)

Common Features

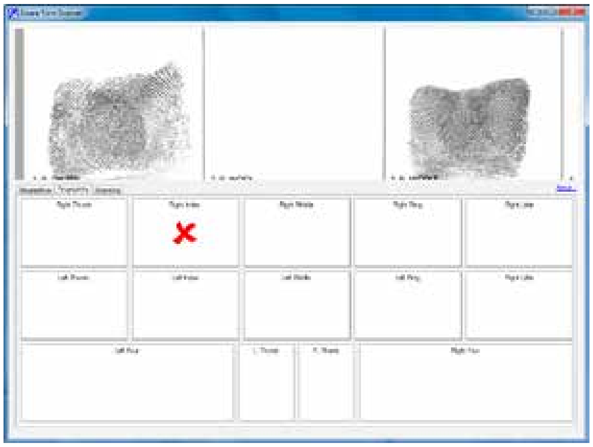
- FBI-certified card scanning solution
- Lossless JPEG 2000 compression of full card images (for Type-16 records)
- WSQ compression (for Type-4/14 records)
- Sequence checking
- Fingerprint image quality scoring
- Parsing, creation, and validation of ANSI/NIST-ITL 1-2011 (and earlier) Type-4, Type-14, and Type-16 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™

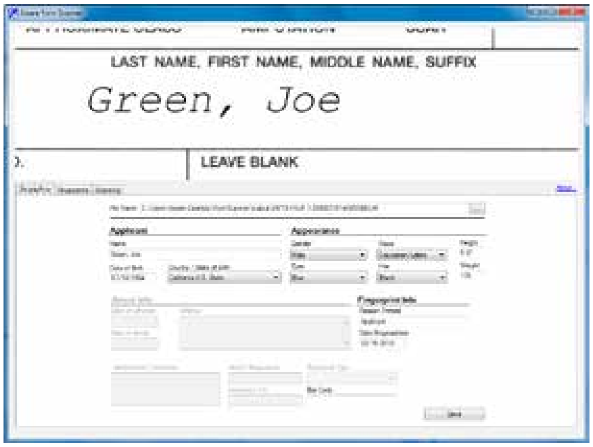
FormScannerSE is a software application designed to assist the process of scanning and processing of fingerprint cards and forms. Used with off-the-shelf consumer-grade flatbed scanners, it utilizes three Aware SDKs: AccuScan, NISTPack, and Sequence-Check, and is FBI certified.

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 hand written 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



LAST NAME, FIRST NAME, MIDDLE NAME, SUFFIX

Green, Joe

LEAVE BLANK

Manual entry of additional field values

FormScannerSE - SWFT Configuration

FormScannerSE is offered as a version preconfigured specifically for "Secure Web Fingerprint Transmission", or SWFT. It includes 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.

BioSP can also be used in a SWFT solution to consolidate SWFT submissions across office that are geographically distributed. It provides browser-based user interface and enrollment, aggregation and management of live scan and card scan submissions, and centralized reporting and administration.

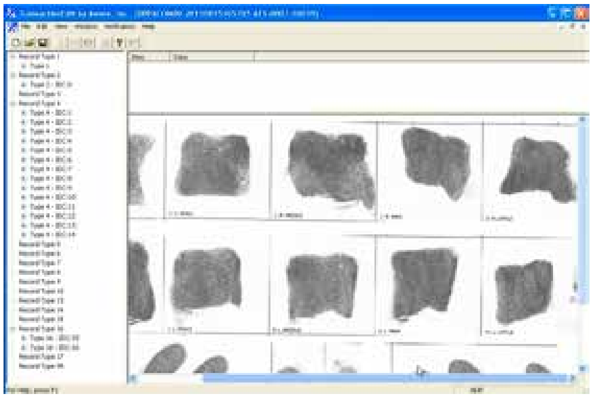
FormScannerMB™

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.

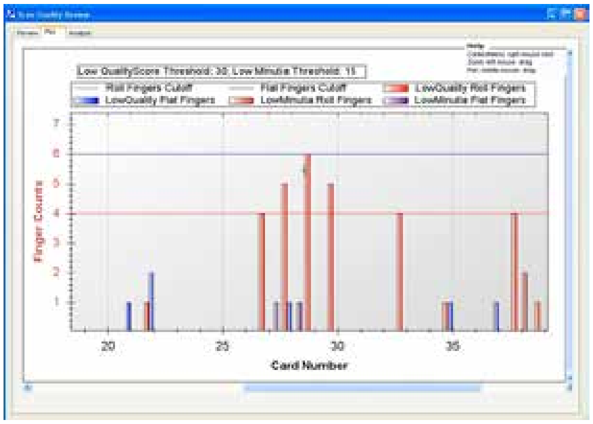
Reports on image quality can be generated during and following the scan of a batch. Configurable quality thresholds can be set, and automatic alerts are generated when thresholds are not met. This is to alert an operator to problems before large quantities of forms are scanned improperly.

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-16 records containing a lossless JPEG 2000 compressed image of the front and back of each card can optionally be included.

The figure below illustrates how both applications can be used to fulfill all workflow requirements for a full high-volume digitization and data entry process. In this scenario, FormScannerMB is first used to batch-scan cards automatically categorize and quarantine files with quality problems. FormScannerSE is then used to manually enter metadata and perform rework on each card that has been scanned using FormScannerMB.

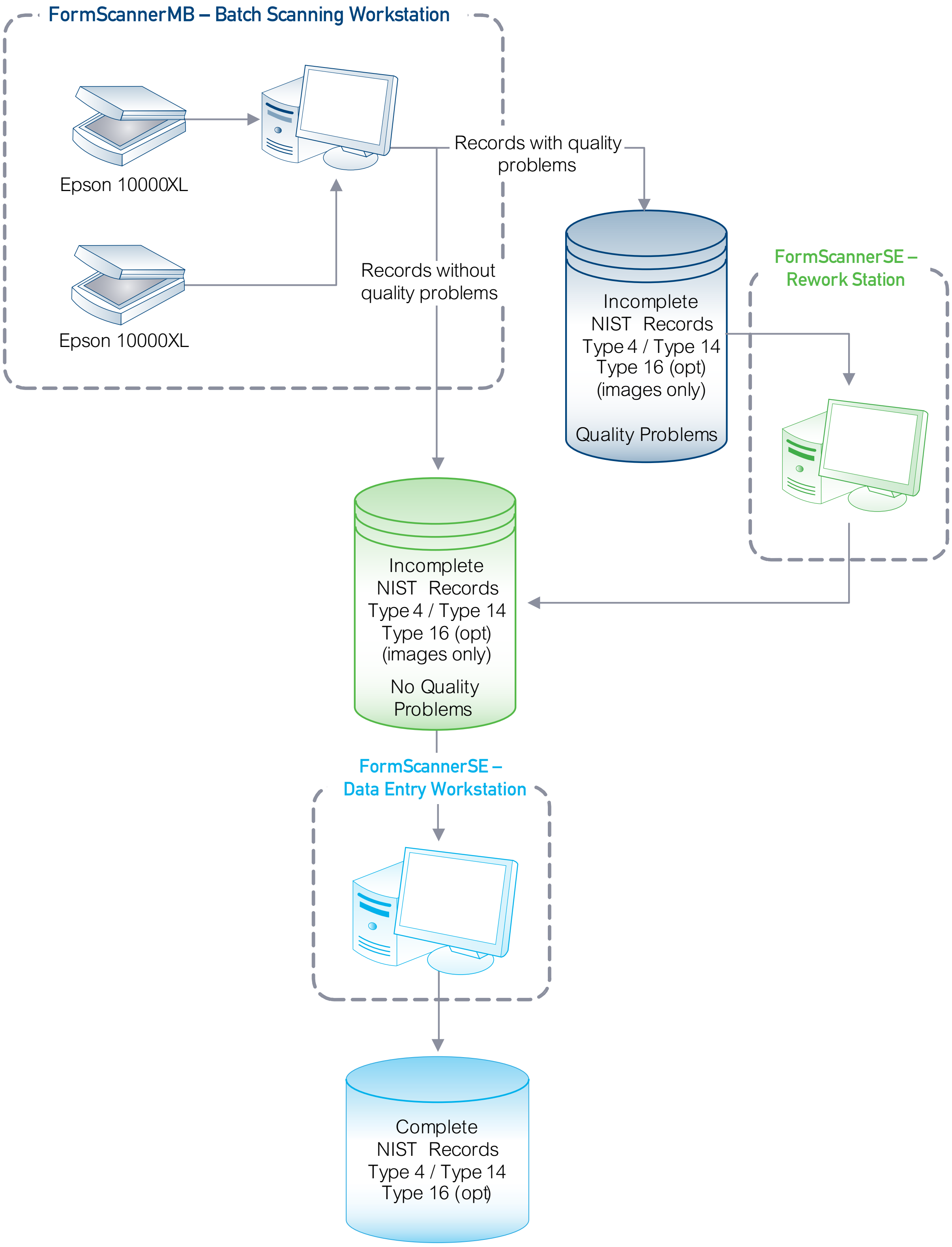


File viewer



Low QualityScore Threshold: 30; Low Minutia Threshold: 15

Batch quality reporting


FormScannerMB – Batch Scanning Workstation
Epson 10000XL
Epson 10000XL
Records with quality problems
Records without quality problems
Incomplete NIST Records Type 4 / Type 14 Type 16 (opt) (images only)
Quality Problems
FormScannerSE – Rework Station
Incomplete NIST Records Type 4 / Type 14 Type 16 (opt) (images only)
No Quality Problems
FormScannerSE – Data Entry Workstation
Complete NIST Records Type 4 / Type 14 Type 16 (opt)

FormScannerMB/SE workflow

FormScannerSWFT™

Software Application for Fingerprint Card Scanning and Conversion to NIST Records for SWFT Submissions

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-16 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 hand written 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.

Functionality Summary

For manual, single card "scan and entry":

- Manual, assisted data entry
- NIST record creation
- FBI-certified card scanning solution
- Lossless JPEG 2000 compression of full card images (for Type-16 records)
- WSQ compression (for Type-4/14 records)
- Sequence checking
- Fingerprint image quality scoring
- Parsing, creation, and validation of ANSI/NIST-ITL 1-2011 (and earlier) Type-4, Type-14, and Type-16 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

For file rework:

- NIST record parsing
- Crop region adjustments
- Sequence error correction
- NIST record output
- Card orientation check

OTHER RELEVANT PRODUCTS

Universal Registration Client (URC) is an enrollment application available in a SWFT version that is preconfigured to perform live scan for SWFT submission instead of card scan. The output is the same, but can be used with a certified live scan device to collect and process high-quality fingerprint images. URC includes CaptureSuite fingerprint image capture and processing libraries to perform quality-based autocapture, image quality scoring, sequence checking, certified WSQ image compression, and NIST formatting.

BioSP can also be used in a SWFT solution to consolidate SWFT submissions across offices that are geographically distributed. It provides browser-based user interface and enrollment, aggregation and management of live scan and card scan submissions, and centralized reporting and administration.

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).

Forensic Workbench

Software Application for Assisted Categorization, Processing, and Formatting of Biometrics

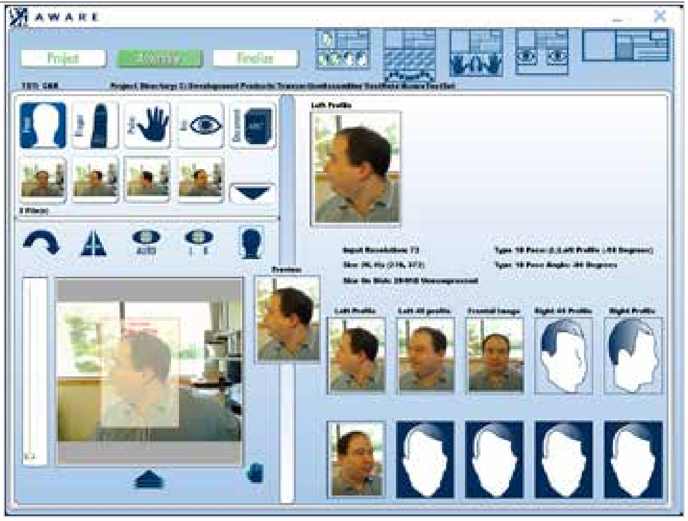
Forensic Workbench is a software application that utilizes several Aware SDKs for the categorization, processing, and standards-compliant formatting of biometric images and demographic data. The primary function of the application is the easy assembly of disparate biometric imagery and text into a standard-compliant data structure, such as ANSI/NIST-ITL 1-2011 (and earlier), FBI EFTS, and DoD EBTS.

Forensic Workbench provides the operator the ability to organize a collection of biometric and demographic images and text files. The basic capabilities include:

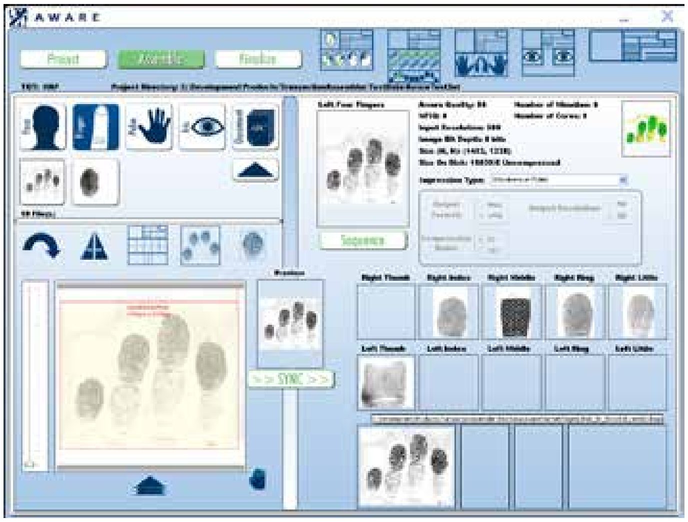
1. **Categorization of data into face, finger, iris, and documents,**
2. **Processing of finger face and iris imagery to specifically label each image and sub-image as facial frontal or other profile, and fingerprint as to its source finger,**
3. **Measurement and reporting of image quality metrics for each categorized and labeled sub-image,**
4. **Generation of an ANSI/NIST-ITL-compliant output file (e.g. DOD EBTS 1.2, Interpol 4.x, FBI EFTS), and**
5. **Modification of the data within an existing EBTS file.**

The first operation in the application workflow is to identify a project directory; all supported files within this directory are loaded. The operator can then categorize each image (i.e. label it as a finger, face, iris, or document). Once the categorization is complete, image type-specific operations may take place.

Forensic Workbench can display and process facial and fingerprint imagery. 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 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



Step 1 – Data Selection. The left side shows the raw biometric data yet to be processed. The right side shows biometric data the operator has selected for processing.



Step 2 - Assembly. 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.

with its source and impression type (live scan, ink, rolled, plain) and its quality reported (Aware's QualityCheck™ and NFIQ). 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 via NISTPack prior to generation of the file.

Biometric processing encompasses the processing of fingerprint, facial and iris biometrics. These capabilities are provided by the following COTS products:

SEQUENCECHECK™ processes fingers from sets of multi-finger enrollments (2-10 fingers) to make the following quality determinations:

- **Locates single or multiple fingers within an image or document, segments them (cuts them out) and indicates the location of the prints to an operator through graphical bounding box overlays.**
- **If the same finger was captured more than once when both rolls and flats are collected,**
- **If a finger was captured out of sequence,**
- **If the wrong hand was captured, and**
- **If fingers from a four-finger image are missing.**
- **SequenceCheck includes a robust multi-finger and hand segmentation to extract individual fingers or hand sections from multi-finger or full hand images.**

PREFACE™ is a facial image analysis software engine that is designed to test and format a facial image so that it is compliant with ANSI/INCITS-385 “Face Recognition Format for Data Interchange.” PreFace is configurable to support other facial image formats including the ISO/IEC equivalent of INCITS 385 (ISO/IEC 19794-5) and NIST Best Practices for Mug Shots. PreFace includes facial image autocapture and camera control for several commercially available cameras.

PreFace provides Forensic Workbench with the ability to auto find a frontal face within a document or an image. It identifies the major facial features, analyzes the face for standard compliant quality assurance. Additionally, it provides cropping/sizing, rotational correction and formatting so that the image can be more appropriately structured for human or automated identification.

Standard Compliant Data Structuring and Validation involves creating a data object that complies with the master standard (ANSI/NIST-ITL 1-200x) and the domain standards (DoD, Interpol, FBI) and checking/validating that each data element meets the detailed requirements of each specification. These capabilities are provided by the following COTS products:

NISTPACK™ is a software toolkit that provides the ability to read/write/edit and validate biometric data that must be compliant with ANSI/NIST-ITL 1-2011 (and earlier). NISTPack is configurable to support all agency specific implementations of this ANSI/NIST standard including the FBI EFTS, the DOD EBTS, as well as the international implementations and those of the individual US states.

NISTPack is used by Forensic Workbench to create the final, standard compliant, interchangeable data structure which enables the original raw biometric data to be searched against a facial, finger, or iris matcher.

Aware WSQ1000™ is an FBI-certified fingerprint compression engine. It provides WSQ compression for 500 ppi finger images and JPEG 2000 compression that meets the FBI Profile for 1000 PPI Fingerprints. Aware WSQ1000 transcodes 1000 ppi JPEG 2000 images to 500 ppi WSQ format to support systems that accept only the 500 ppi data. Aware WSQ1000 is the defacto standard for systems that required highly optimized, highly error resilient and fully compliant WSQ finger and palm image encoding (compression).

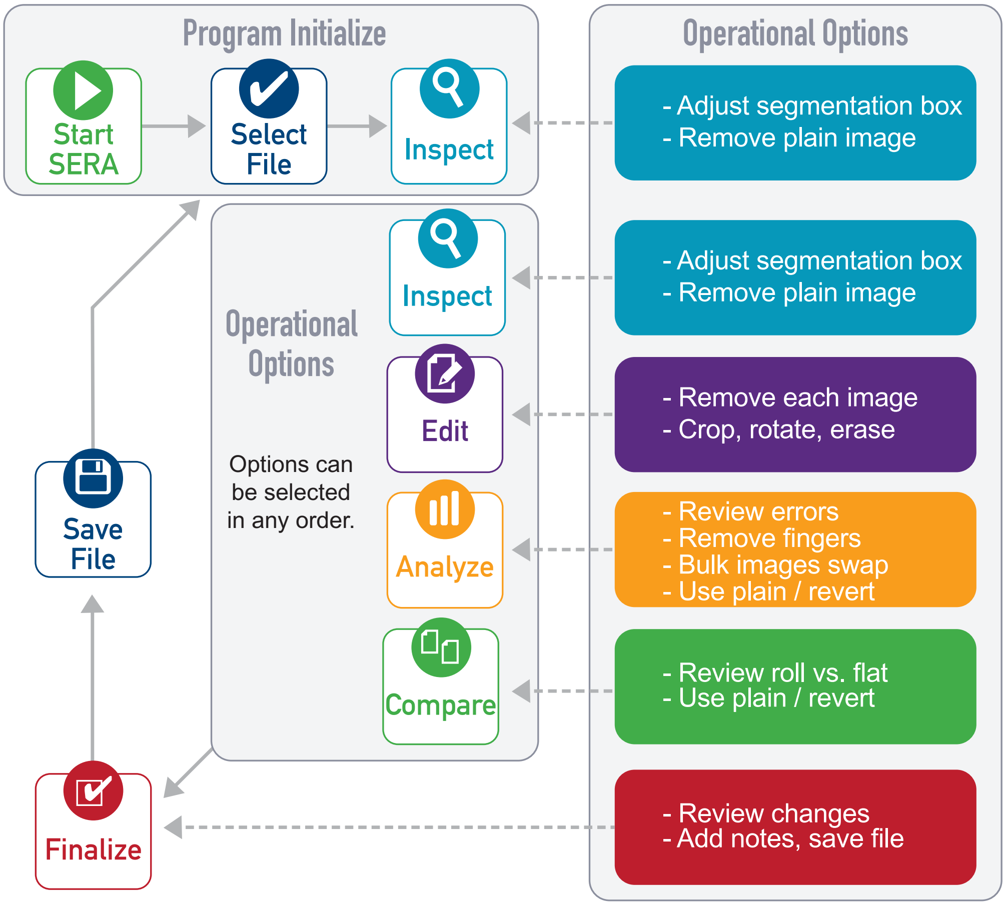
SequenceWorkbench™

A workstation application for repairing 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 in a transaction (both Type-4 and Typ-14) and report sequence errors to the operator. It allows the operator the ability to:

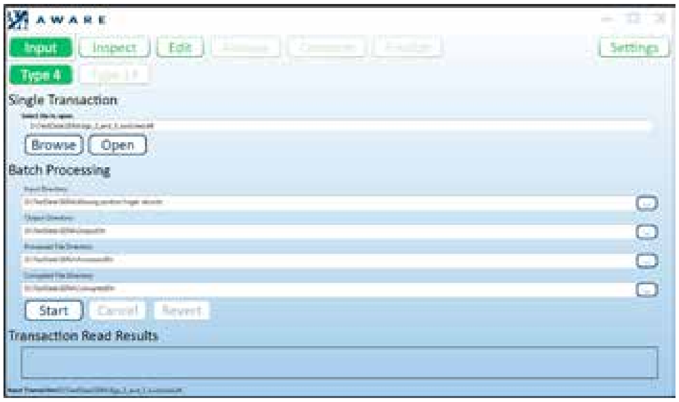
- work with both type 4 and type 14 fingerprint images
- edit individual fingerprint images (erase , rotate, adjust brightness and contrast)
- compare fingerprint images (include zooming and panning)
- remove individual fingerprint images
- generate individual fingerprint images from multi-finger slap 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

SEQUENCEWORKBENCH WORKFLOW



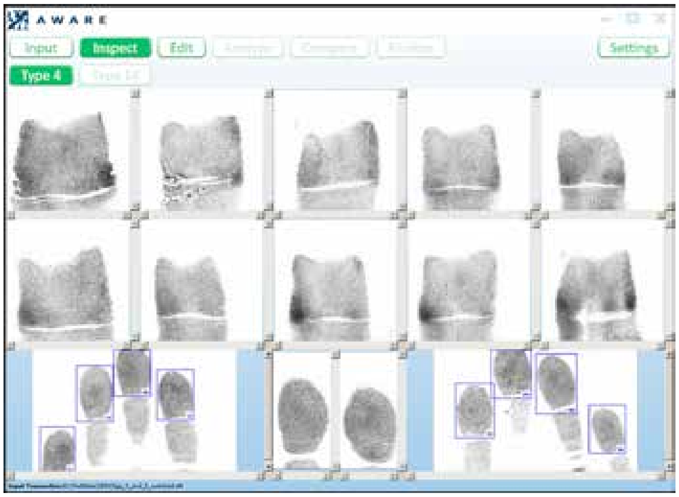
INPUT SCREEN

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.



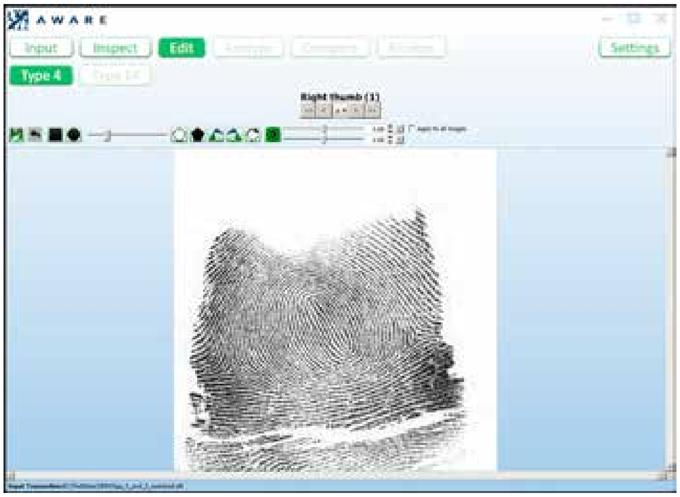
INSPECT SCREEN

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.



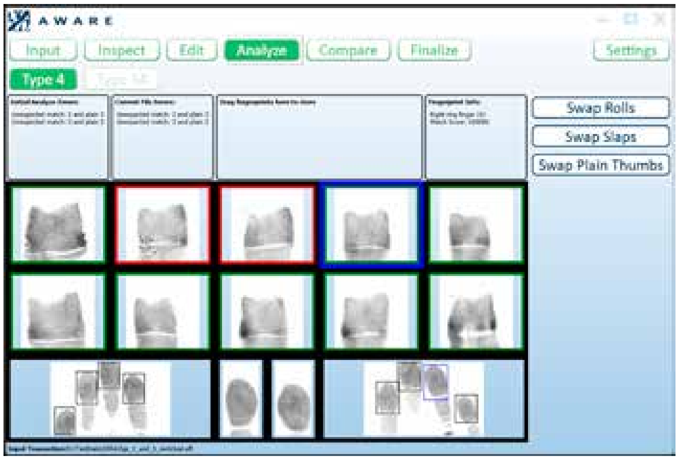
EDIT SCREEN

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.



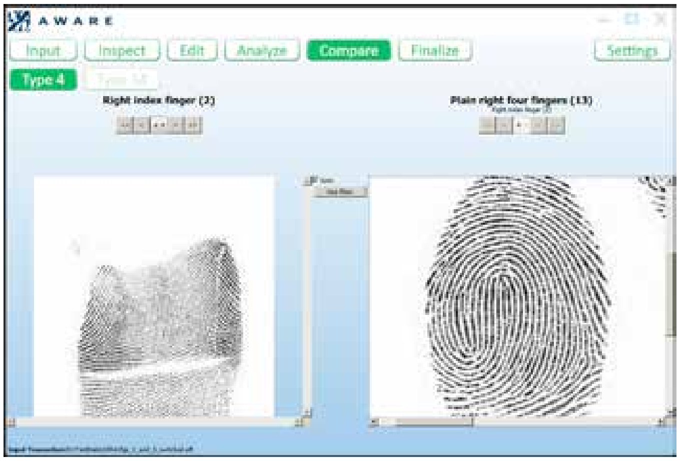
ANALYZE SCREEN

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.



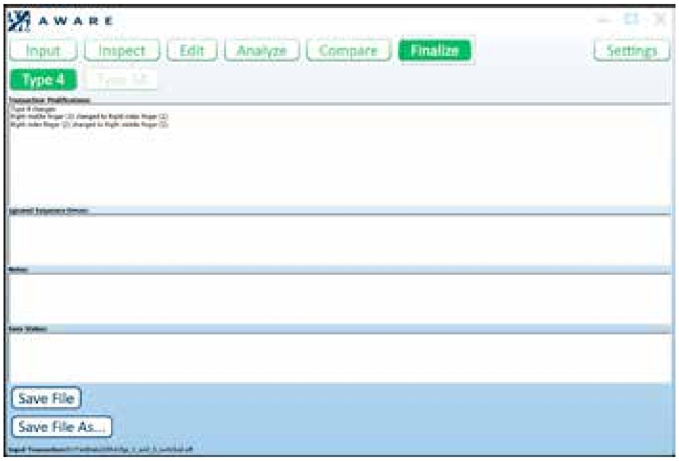
COMPARE SCREEN

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.



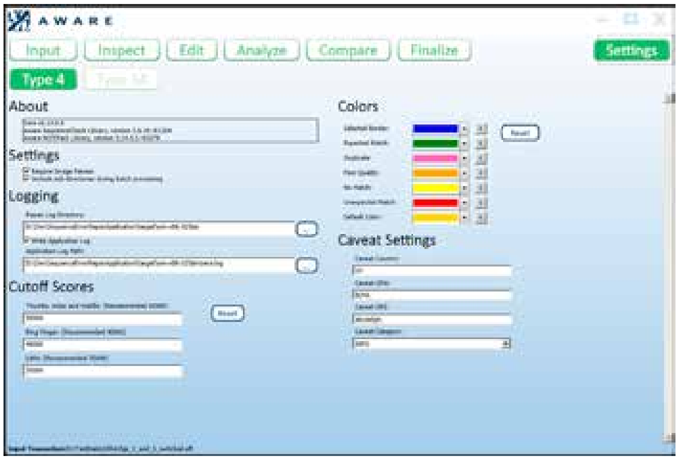
FINALIZE SCREEN

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.



FaceWorkbench

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

The proliferation of digital photography and facial images have made them more useful in law enforcement. FaceWorkbench is an application for analysis and processing of candidates returned as a result of a facial biometric search. The workflow of the application facilitates submission of a facial image for search to a facial recognition system. These systems (including FBI face matching services) often return a list of candidates, as opposed to a “lights out” result. FaceWorkbench provides a user interface and systematic workflow to enable an analyst to analyze and process the candidates returned from the search.

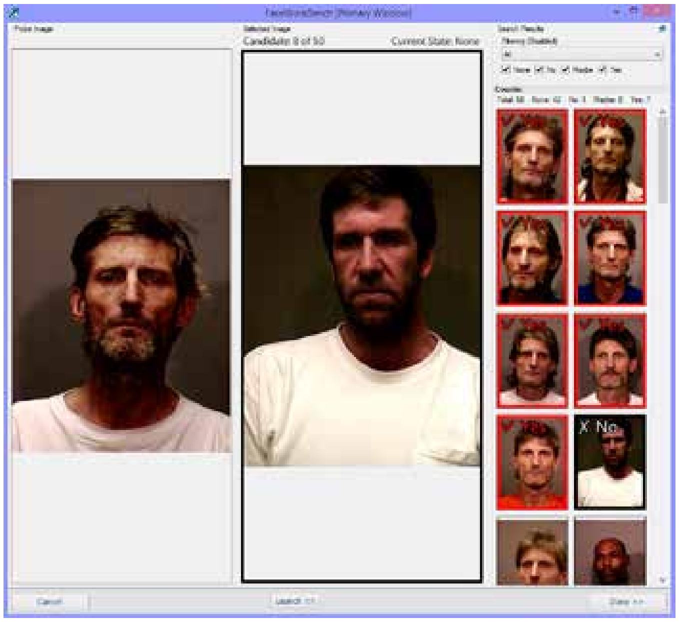
The workflow emulates an email client, with an inbox and outbox of searches in various stages of progress. For a given search result, each candidate can be identified by the analyst as a match or non-match. Advanced tools are provided to enable the user to assess the likelihood of a match between the probe and each candidate.

For example, the features of the facial images of the probe and candidate are automatically located and used to align the images. An analyst can also manually adjust eye locations to better align the images. There are advanced image enhancement functions, including swipe bars, color and other enhancements, and a synchronized, configurable magnifier. Comparison tools allow the images to be overlaid and blended, split, stacked, and checkered.

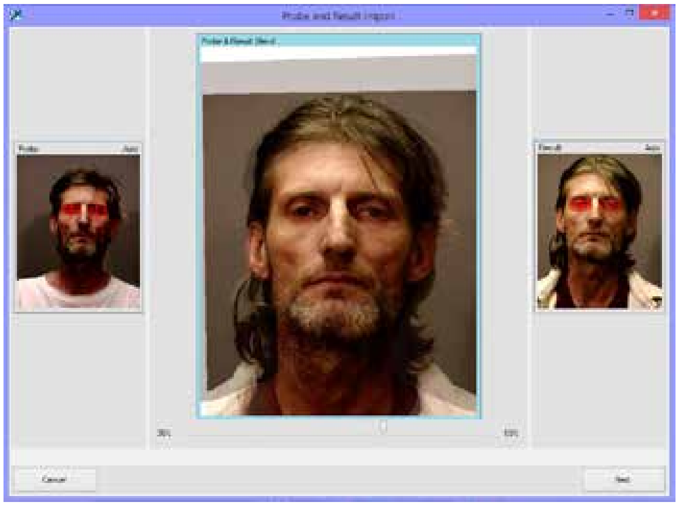
As with fingerprints, standards are required that define the use of digital face images as evidence, such as those drafted by FISWG. A key feature of FaceWorkbench is its integration of forensic facial analysis standards into the workflow. The user is prompted to perform best practices, and keep track of which practices have been performed.

FEATURES & FUNCTIONALITY

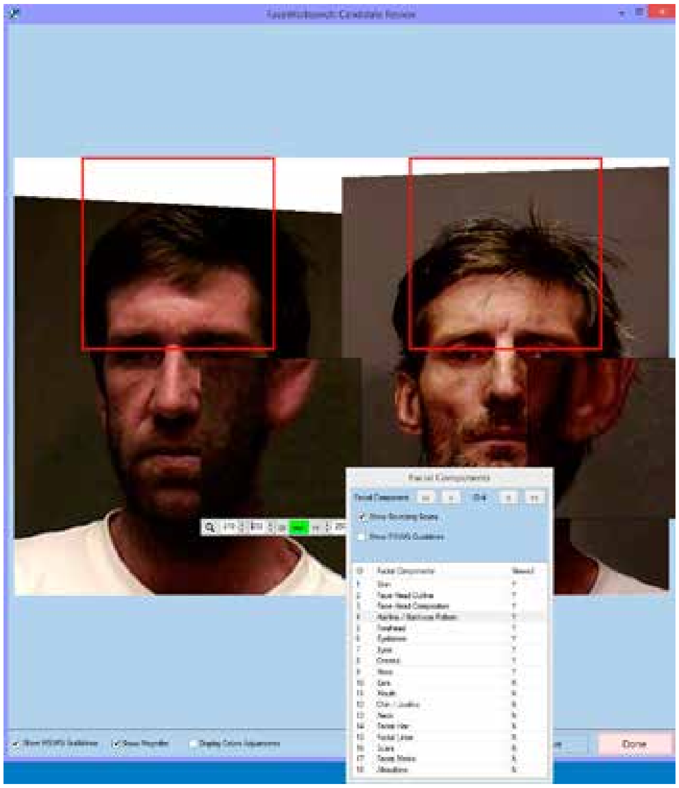
- Management of FBI mugshot search results
- Forensic analysis and comparison of facial images
- Advanced image analysis and comparison tools
  – Adjustable blend
  – Swipe bar
  – Synched magnifier
  – Color filters (red, green, blue, cyan, magenta, yellow)
  – Brightness, saturation, contrast, inversion
- Intuitive “email client” workflow and features
- Integrated examiner training features and best practices



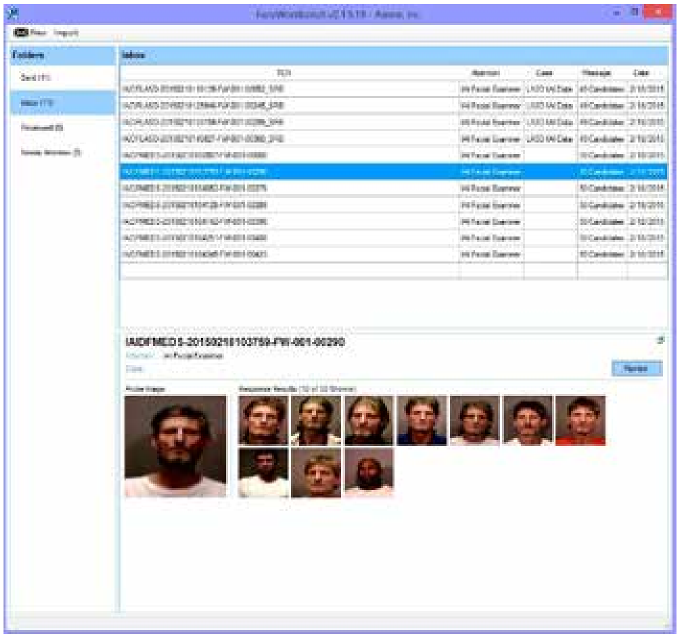
Review and categorization of results candidates as Yes, No, Maybe



Assisted feature alignment with blend slider



Synchronized magnifier for feature comparison
and standards-guided feature review

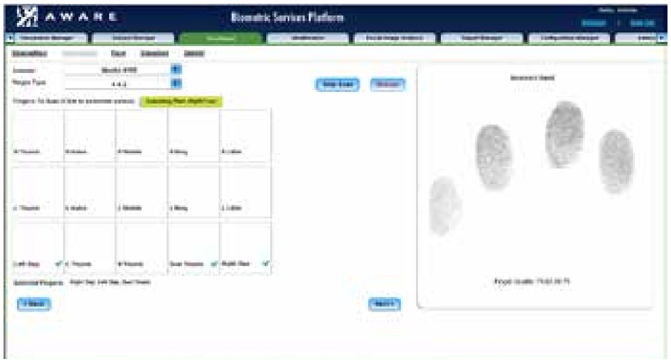


Mail client styled workflow, with inbox
preview of search results

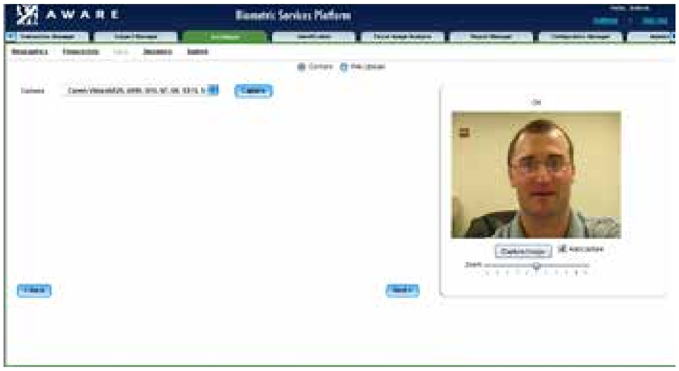
WebEnroll

Browser-Based Application for Biometric Enrollment with Autocapture and Hardware Abstraction

WebEnroll is a browser-based enrollment application that utilizes BioComponents for capture of biographic data, fingerprints, facial images, and iris images. BioComponents are Java applets that implement Aware's FastCapture, PreFace, and IrisCheck software products and associated hardware abstraction libraries. Each applet provides a user interface and capture workflows to perform advanced biometric image autocapture as well as capture device hardware abstraction. Once images are captured, they are submitted to Biometric Services Platform (BioSP™), where configurable workflows and modular software applications are used for processing, routing, and storage of each transaction. Biometric verification and/or identification using either the BioSP Fingerprint Identification Module, or one of several third-party matchers integrated with BioSP, or an external matching service.



Biometric enrollment in a browser application - fingerprints



Biometric enrollment in a browser application - face

FEATURES AND FUNCTIONALITY

- **Abstraction of fingerprint, face, and iris capture peripherals**
- **No personally identifiable information (PII) stored on the workstation**
- **Most recent applet versions distributed and used automatically**

BioComponents™

Modular, Configurable Biometric Enrollment Software Components with "Micro-Workflows" and User Interfaces

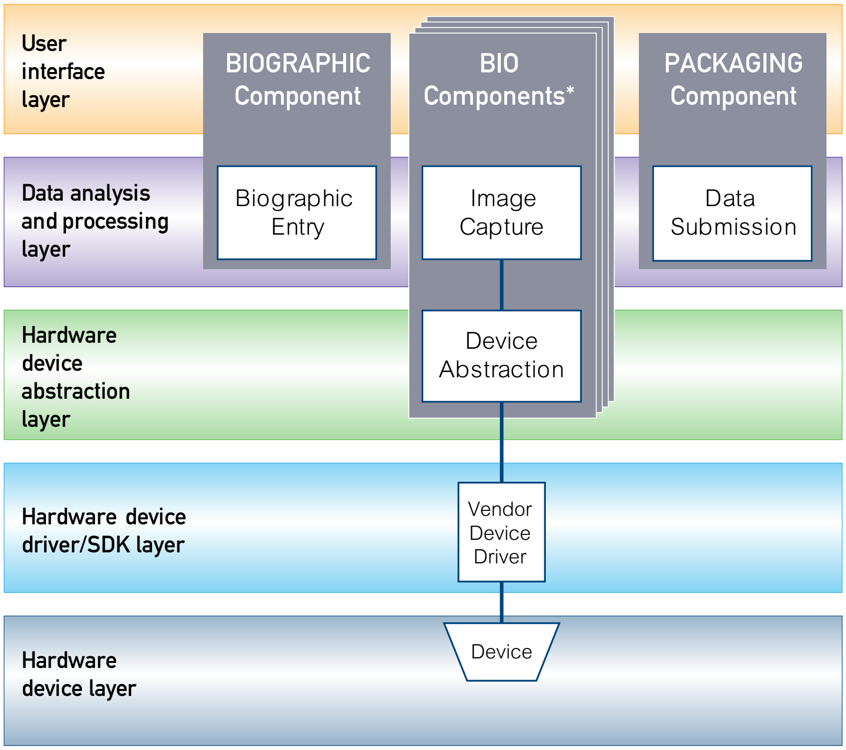
BioComponents comprise Aware's newest biometric enrollment application framework, and include a family of independent biometric enrollment software components. Each BioComponent is designed to enable rapid implementation of a robust .NET or browser-based biometric enrollment application with a high degree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

Most BioComponents utilize APIs from Aware's well-established and field-proven SDKs for underlying biometric functionality. Each Component is packaged as either a Java applet or .NET user control, and can be used independently within either a Microsoft C#/.NET or Java application, or in a variety of web environments (ASP.NET, JSP, HTML). BioComponents can operate within Aware's Universal Registration Client (URC™) .NET enrollment application.

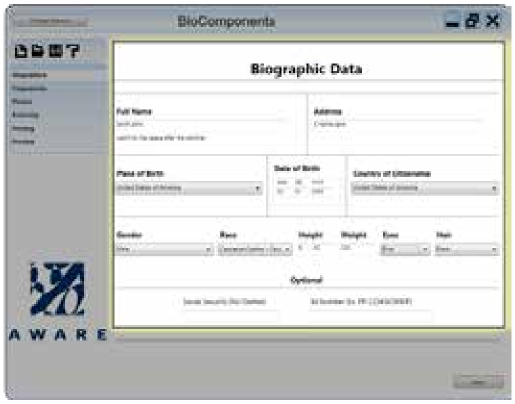
BioComponents are particularly well-suited for supporting multiple different biometric enrollment applications from a single platform, with each having some different functionality requirements and constraints. Using BioComponents provides common capabilities, maintenance, and support, and yet enables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

BioComponent	Functionality
BiographicComponent	Biographic and textual data entry
FingerprintComponent	Fingerprint capture and scanner abstraction
FaceComponent	Face capture and camera abstraction
IrisComponent	Iris capture and camera abstraction
TravelDocComponent	Passport reading and authentication
ScanningComponent	Scanning of fingerprint cards and other forms
PrintingComponent	Printing of fingerprint cards and other forms
SignatureComponent	Handwritten signature capture and signature pad abstraction
PackagingComponent	Data formatting, compliance checking, and submission

BioComponents Framework

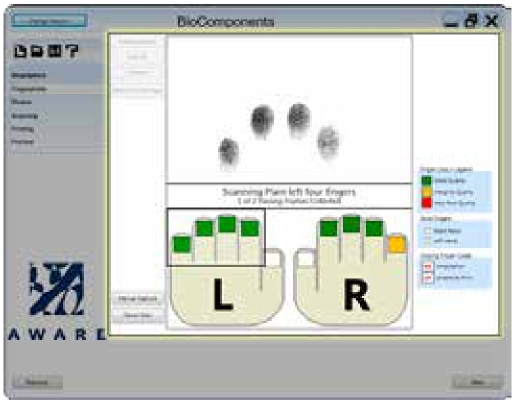


BiographicComponent



BiographicComponent enables highly configurable data entry via its user interface. It utilizes a configuration file that defines the data entry boxes (size, shape, color, label, etc.) and the data that each entry box is designed to accept. A separate user interface called Form Designer is used by the application designer to layout and design the look, feel, and behavior of the Component. Together, the Form Designer and BiographicComponent are designed to enable update, enhancement, and modification to the application without having to make significant changes to the application code. The configuration file allows for all displayed widgets to be specified and validated and how they should be validated.

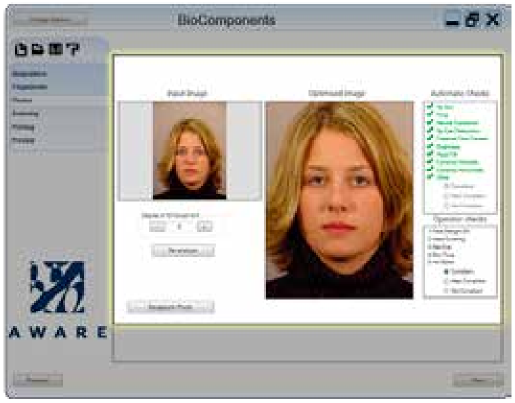
FingerprintComponent



Fingerprint Component implements libraries from three Aware SDK products: FastCapture with 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)**

FaceComponent

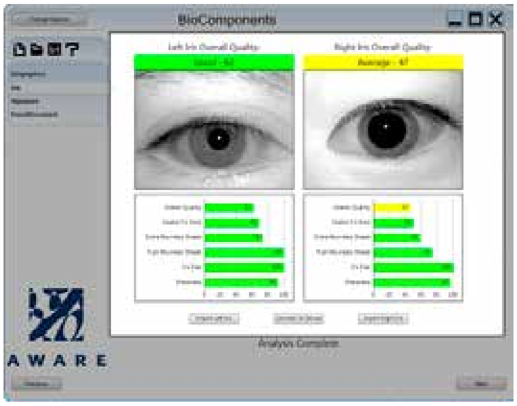


FaceComponent is used to automatically capture biometric facial images according to U.S. and international biometric standards (e.g. ISO/IEC 19794-5). It includes libraries from the PreFacewith Camera API SDK. It has its own user interface and performs:

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

FaceComponent can also be used to collect side profiles and SMT (scars, marks, tattoos).

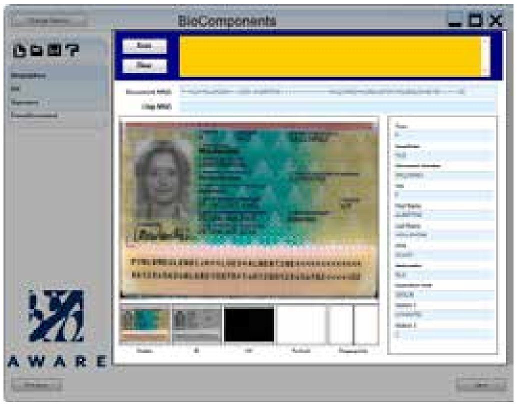
IrisComponent



IrisComponent is used to perform automated capture, segmentation, and quality scoring of biometric iris images according to the ISO/IEC 29794-6 standard for iris image quality. It uses libraries in the IrisCheckwith IrisCam API SDK. IrisComponent also enables plug-and-play operation with several iris cameras. It has its own user interface and performs the following functions:

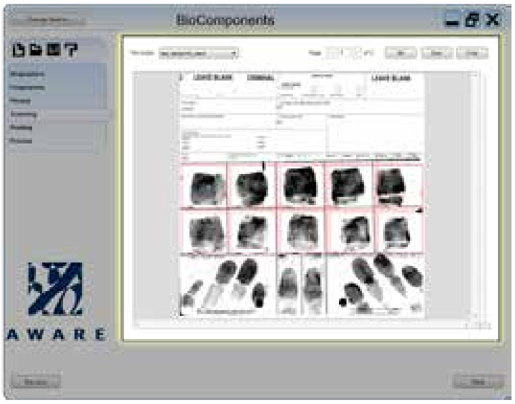
- Specularity removal
- Pupil segmentation
- Iris segmentation
- Parametric curve fitting
- Eyelash detection
- Shadow detection

TravelDocComponent



TravelDocComponent performs authentication of travel documents and credentials such as passports and driver's licenses. It utilizes third-party document authentication software and operates with several third-party document scanners.

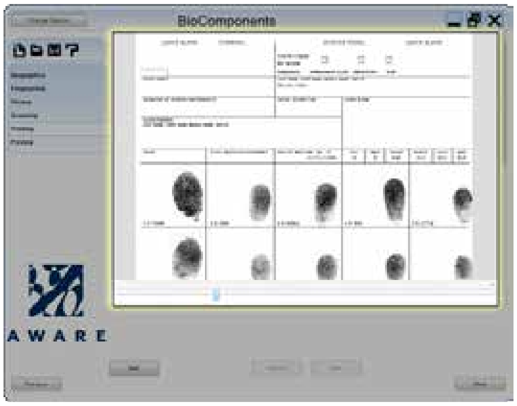
ScanningComponent



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.

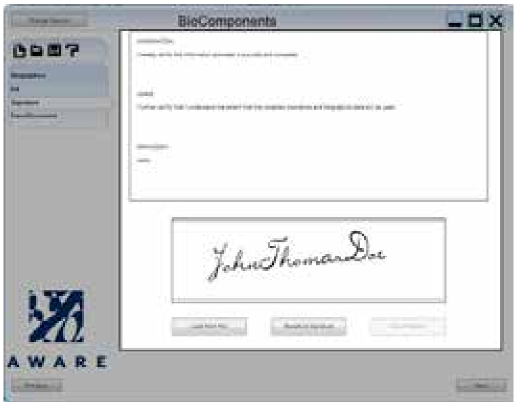
PrintingComponent



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

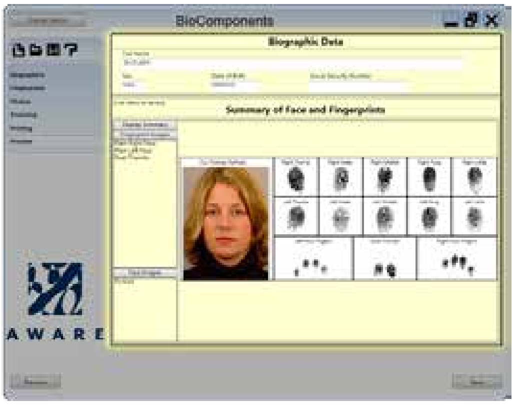
- **Parsing of fingerprint images from transactions, such as EFTS**
- **Decompression of fingerprint images**
- **Mapping of text and images to correct location on the form**
- **Printing of card graphics such as lines and labels**
- **Generation of 1-bit dithered image to simulate gray-scales**
- **Creation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

SignatureComponent



SignatureComponent is used to collect handwritten signature images from an electronic signature pad. It includes a user interface, supports several market-leading electronic signature pad devices, and performs data formatting and validation of the output according to the ANSI/NIST-ITL 1-2011 standard for Type-8 records.

PackagingComponent



PackagingComponent 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:

- **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**

PackagingComponent can then save or submit the updated transaction.

Biometric Services Platform (BioSP™)

A Modular, Service-Oriented Biometric Middleware and Workflow Server

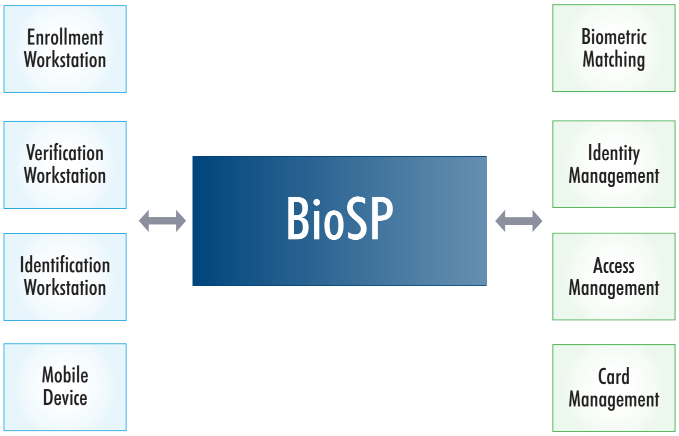
Aware's Biometric Services Platform (BioSP) is a service-oriented application server platform used to enable advanced biometric data processing and management functionality in an Enterprise Service Bus (ESB) architecture. BioSP is well suited for applications that require the collection of biometrics 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-sou Aware's Biometric Services Platform (BioSP) is a service-oriented application server platform used to enable advanced biometric data processing and management functionality in a web services architecture. 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 J2EE-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.



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

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.

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 J2EE 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 via YAMI technology, 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 base 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.

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

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.

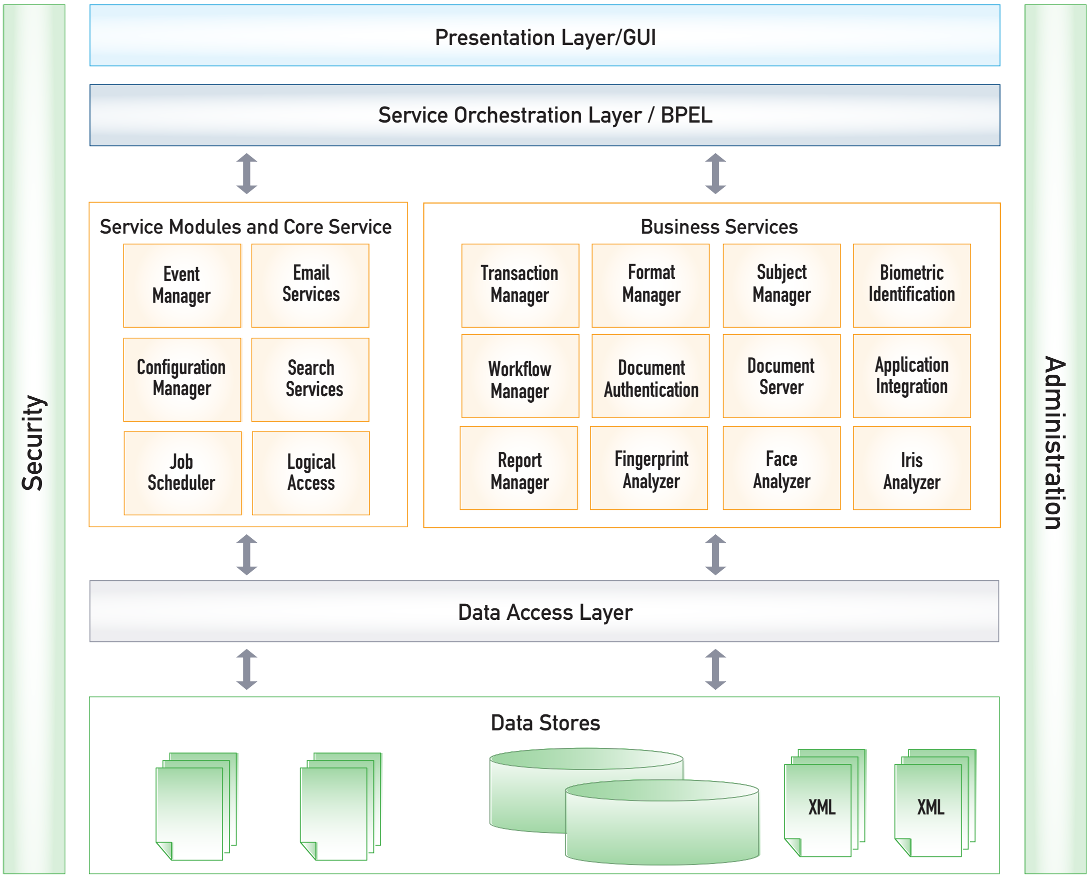
BioSP supports the concept of roles. A user with a given role is given permission to access a resource in a specific manner. For example, a user may be assigned to a role that allows them to see a list of transactions but not to see the individual NIST fields in the transactions. Another user may have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

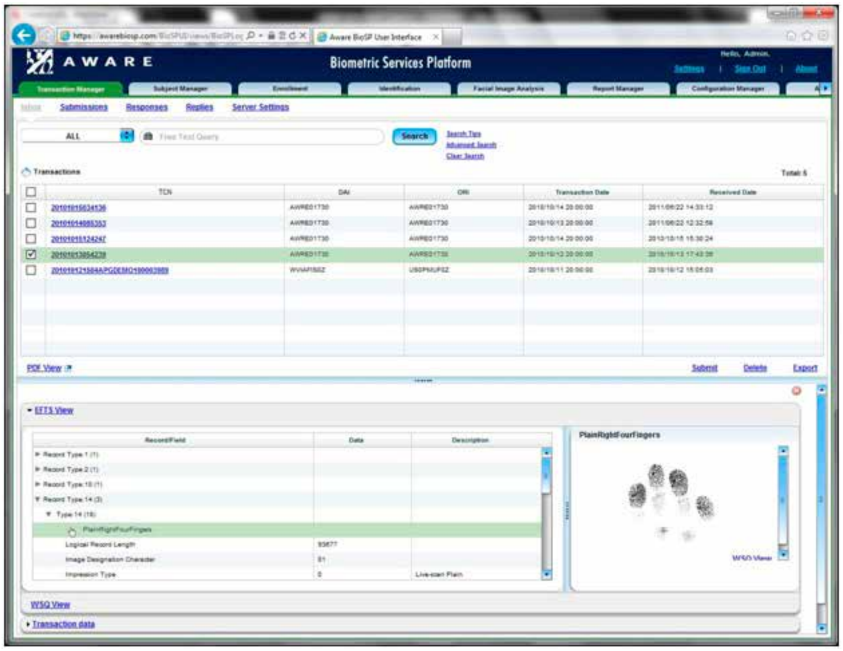
BioSP supports the concept of groups. A group is a logical grouping of users. This allows BioSP to support functionality such as dividing users into groups. Groups are independent of roles; a user can have multiple roles and belong to multiple groups.

Other security-related features provided are:

Improved searching, sorting, and filtering of transactions, including searching, sorting and filtering based on submitting agency

- **Creation of users and groups that can see all transactions for a given agency or group**
- **Denying access to a view based on user's access permission**
- **Role based access to transaction field viewing**
- **Prevention of password reuse**
- **Minimum password age before change is allowed**
- **Forced password change after a specified number days**
- **Account disabling after a specified number of failed logins for a specified number minutes.**
- **Account locking after a specified number days of inactivity**





Biometric Services Platform

Transactions

Total: 5

□	TCN	DAI	ORI	Transaction Date	Received Date
□	20101015034136	AWRE01730	AWRE01730	2010/10/14 20:00:00	2011/06/22 14:33:12
□	20101014085353	AWRE01730	AWRE01730	2010/10/13 20:00:00	2011/06/22 12:32:58
□	20101015124247	AWRE01730	AWRE01730	2010/10/14 20:00:00	2010/10/15 15:30:24
☑	20101013054239	AWRE01730	AWRE01730	2010/10/12 20:00:00	2010/10/13 17:43:38
□	201010121504APGDEMO100003989	WVIAFIS0Z	USDPMUFSZ	2010/10/11 20:00:00	2010/10/12 15:05:03

Record/Field	Data	Description
▸ Record Type 1 (1)		
▸ Record Type 2 (1)		
▸ Record Type 10 (1)		
▾ Record Type 14 (3)		
▾ Type 14 (18)		
PlainRightFourFingers		
Logical Record Length	93677	
Image Designation Character	01	
Impression Type	0	Live-scan Plain

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.

BIOSP CORE

BioSP Core provides the central infrastructure services shared across BioSP modules and business processes. The 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.

TRANSACTION MANAGER

BioSP Transaction Manager provides services for building transaction workflows between multiple disparate systems, including enrolment 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.

Transaction Manager provides broadcast capabilities, whereby a single input transaction may be distributed to multiple external systems upon submission. In turn, Transaction Manager consolidates responses from multiple external systems that relate to a single, original submission, and manages this consolidation until all responses have been received for a given transaction.

Transactions received may be archived for reporting and resubmission in the event a submission fails. The resubmission logic within Transaction Manager integrates with workflows and the BioSP Core Job Scheduler to manage retry of failed submissions. Each destination has a unique resubmission configuration managed by and stored in Transaction Manager, such that different rules can be applied for resubmission to different systems. Transaction Manager offers a browser-based interface for searching and viewing transaction content and status.

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 enrolment 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.

Subject Manager receives enrolment data and populates its data stores and search indexes, providing services for managing new and existing identities, including create, delete, retrieve, and update of subject data. Subjects, or identities, are archived in the subject manager data store and indexes for field- or contextual-based searching. Biometrics are stored in image or template form for integration with internal or external matching systems and other business processes requiring biometrics. Subject Manager offers a browser-based interface for viewing and searching subject entry content.

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.

Format Manager can build these data structures from the raw biometric and textual metadata or it can parse one type of data structure and convert it to another. Examples of this formatting include:

- **Creation of ANSI/NIST, FBI EFTS, DoD EBTS, PIV, or ICAO data structures from raw enrolment data**
- **Creation of card personalization requests according to vendor-specific formats**
- **Conversion between FBI EFTS and DOD EBTS**
- **Conversion between Interpol ANSI/NIST and a specific country format**
- **Conversion between binary ANSI/NIST and the XML variant of the standard**
- **Conversion of ANSI/NIST Type-4 or Type-14 finger image records to ICAO DG3 format, ISO/IEC 19794, INCITS 378/381 or FIPS 201 (images or templates)**
- **Conversion of ANSI/NIST Type-10 records to ICAO format (ISO/IEC 19794-5) or FIPS 201 format (ANSI/INCITS 385)**
- **Conversion of WSQ and JPEG 2000 images to JPEG for easy viewing in a browser**
- **Conversion of fingerprint transactions to fingerprint card images in PDF format**

Data is parsed from input transactions in preparation for processing of the data depending on the business rules for a particular workflow. Data from one transaction may be transformed to create another, single transaction. Data may be edited and repackaged in the same or different formats.

A single transaction may also be used to create multiple, differently-formatted results. Multiple inputs may also be merged into a single transaction. Finally, data from disparate sources, be it other transactions, other data files, databases, or text, may be used to create a new transaction.

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.

Aware's Nexa matching algorithms or external matching engines 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.

One-to-one matching compares one or more biometric templates submitted to the matcher with corresponding templates stored in the database, leading to verification of an individual's claimed identity. Common use cases include physical and logical access control applications and match-on-server based biometric verification prior to credential issuance. One-to-many matching is used to compare a set of biometrics with a gallery of subjects with the goal of determining an identity. Inbound biometric data is enrolled to matcher galleries, which are collections of biometric data.

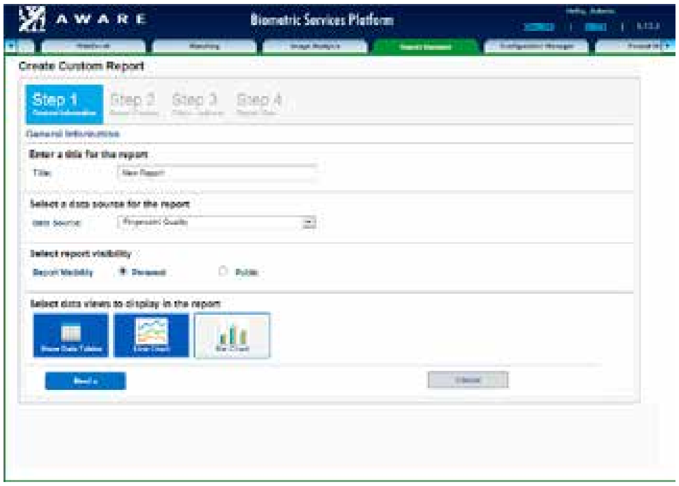
Biometric Identification module supports the matching of standard compliant fingerprint templates (ISO/IEC 19794-2 or ANSI/INCITS 378).

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 enrolment problems, quantify environmental factors, and perform general system performance monitoring and improvements.

All raw data collected for each subject and component (e.g. all ten fingers in a slap/plain impression) is aggregated and processed into OLAP cubes according to selectable parameters. Custom reports are presented that can summarize data in such a way as to enable informed decision making. For example, data might be presented that measures biometric image quality as a function of capture hardware device or operator, and presents summarizing statistics such as averages and standard deviations with automatically identified outliers. A capture device shown to yield average quality scores that are low to a statistically significant degree could indicate that the device is working improperly. Similarly, an operator requiring additional training might be identified. Finally, environmental effects such as humidity or temperature could be correlated to image quality. Output report formats include PDF, comma-separated value (.csv), HTML, and XML/XSL.

Creating a Report



AWARE Biometric Services Platform

Create Custom Report

Step 1 Step 2 Step 3 Step 4

General Information

Enter a title for the report

Title: New Report

Select a data source for the report

Data Source: Fingerprint Quality

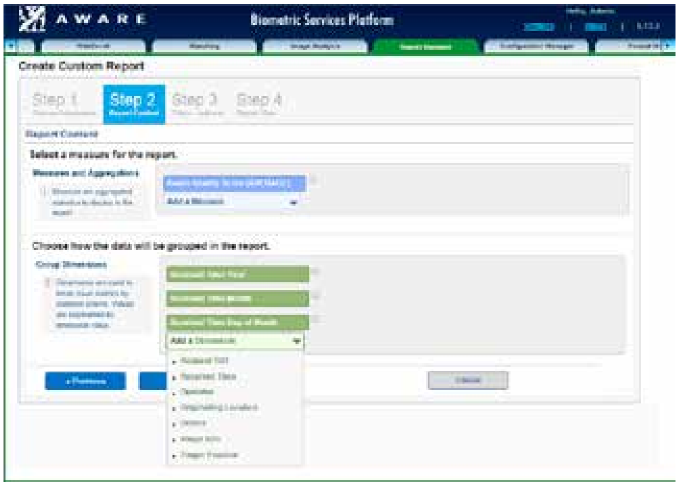
Select report visibility

Report Visibility ● Personal ○ Public

Select data views to display in the report

Show Data Tables | Line Chart | Bar Chart

Next › | Cancel



AWARE Biometric Services Platform

Create Custom Report

Step 1 Step 2 Step 3 Step 4

Report Content

Select a measure for the report.

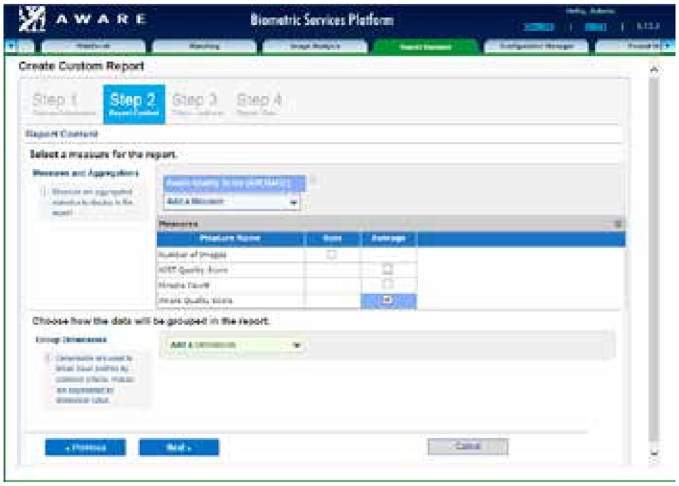
Measures and Aggregations: Aware Quality Score (AVERAGE); Add a Measure

Choose how the data will be grouped in the report.

Group Dimensions: Received Time Year; Received Time Month; Received Time Day of Month; Add a Dimension

‹ Previous | Cancel

Designing a New Report



AWARE Biometric Services Platform

Create Custom Report

Step 1 Step 2 Step 3 Step 4

Report Content

Select a measure for the report.

Measures and Aggregations: Aware Quality Score (AVERAGE); Add a Measure

Measures

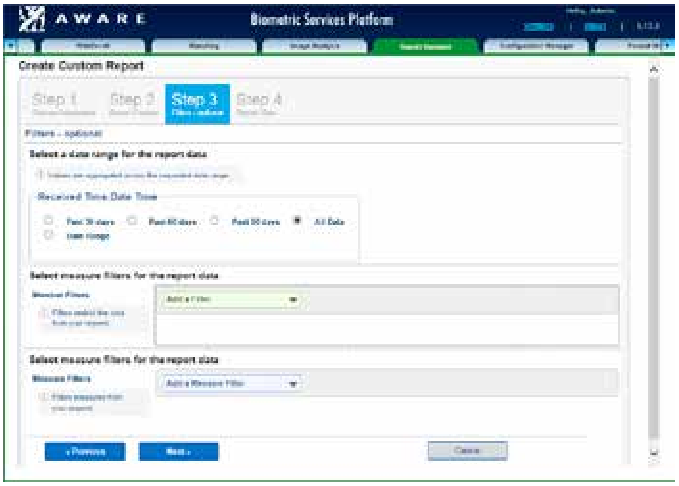
Measure Name	Sum	Average
Number of Images	□	
NFIQ Quality Score		□
Minutia Count		□
Aware Quality Score		☑

Choose how the data will be grouped in the report.

Group Dimensions: Add a Dimension

‹ Previous | Next › | Cancel

Modifying a Report with Filters



AWARE Biometric Services Platform

Create Custom Report

Step 1 Step 2 Step 3 Step 4

Filters - optional

Select a date range for the report data

Received Time Date Time

○ Past 30 days ○ Past 60 days ○ Past 90 days ● All Data ○ Date Range

Select measure filters for the report data

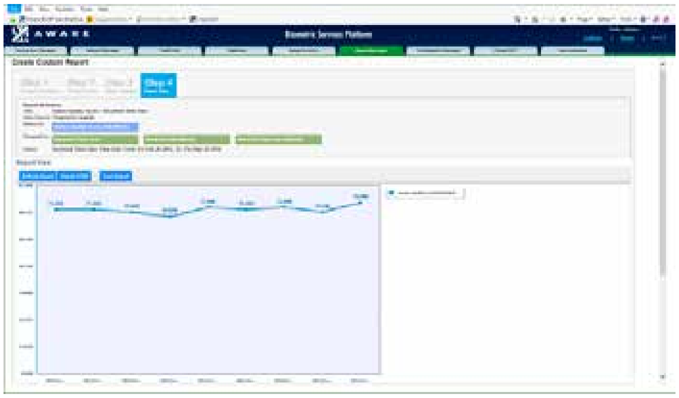
Add a Filter

Select measure filters for the report data

Measure Filters: Add a Measure Filter

‹ Previous | Next › | Cancel

Displaying a Report



AWARE Biometric Services Platform

Create Custom Report

Step 4

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. Some of the functions performed by this module are as follows:

- **Compression ratio calculation**
- **Images noise reduction**
- **Left/right hand identification**
- **WSQ, JP2 or JP2L compression and decompression**
- **Insertion of binary or text comments into images during compression and decompression**
- **Transcoding of JP2, JP2L images to WSQ**
- **Downsampling of fingerprint images**
- **Segmentation and cropping of single fingers from slap images**
- **Calculation of NIST and Aware QualityCheck scores**
- **Sequence checking with match and non-match checking**
- **Light, dark, and invalid image detection**

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 enrolment 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™

Cluster Computing Platform for Scalable Biometric Search and Match

Astra™ is a software platform that performs rapid processing and analysis of large stores of biometrics and other identity data by deploying biometric and text 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.

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, well-supported, and open. Astra is fault-tolerant, 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.

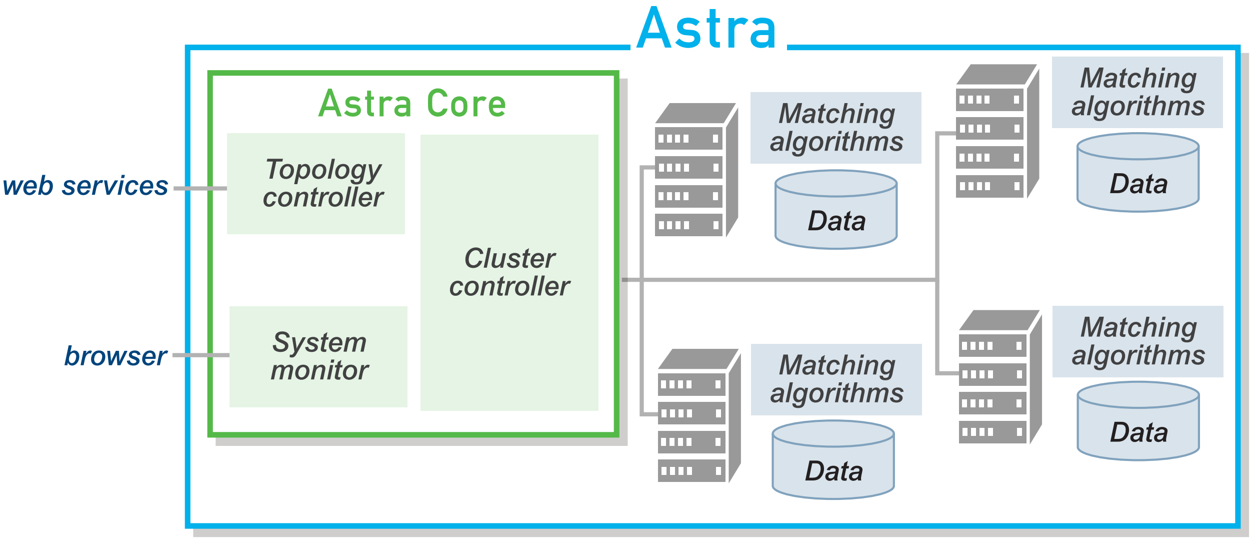
Astra configures a multi-node computing topology and deploys the algorithms and data to each node, then manages the execution of the millions of operations and results in such a way that maximizes the utilization of the machines and processors. The platform is independent of the algorithms in use,

FUNCTIONALITY

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

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



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.

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.

APPLICATIONS

- Public/private cloud-based identity data computing
- High-volume, high-availability biometric authentication
- Large-scale biometric identification and duplicate detection
- Large-scale identity data quality analysis, identity resolution, and link analysis

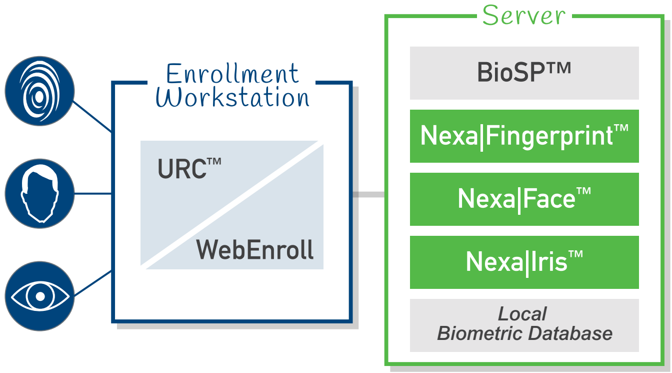
Nexa™

Biometric Search and Match SDKs for Fingerprint, Face, and Iris

Aware's Nexa|Fingerprint™, Nexa|Face™, and Nexa|Iris™ biometric search and match algorithms deliver high accuracy and fast search speeds in SDK packages that are reliable, configurable, and easy to use. They are complemented by a level of technical support that has helped make Aware a trusted provider of high-quality biometric enrolment and workflow 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 configuration tools that help quantify system performance, identify opportunities for improvement, and continuously optimize the system.

Each Nexa SDK can be deployed on a workstation or server, either as a standalone biometric search/match API, or in combination with Aware's other modular, COTS SDKs, applications, and Biometric Services Platform (BioSP™). Aware's SequenceCheck, PreFace, and IrisCheck SDKs can be used in concert with Nexa libraries to perform optional quality assurance and preprocessing for enhanced fingerprint, face, and iris search functionality, respectively.



For large-scale biometric searching and matching, Nexa SDKs can be deployed on the Astra cluster computing platform, optimized for rapid biometric search of extremely large databases, high-volume biometric authentications, as well as identity resolution.

Standalone APIs or a Complete Modular Solution

Each Nexa SDK can be deployed on a workstation or server, either as a standalone biometric search/match API, or in combination with Aware's other modular, COTS SDKs, applications, and Biometric Services Platform (BioSP™). Aware's SequenceCheck, PreFace, and IrisCheck SDKs can be used in concert with Nexa libraries to perform optional quality assurance and preprocessing for enhanced fingerprint, face, and iris search functionality, respectively.

FEATURES

- Well-designed, easy-to-use APIs
- Fully scalable and extensible
- Highly configurable and tunable for performance optimization
- Fully leverages multicore processor power
- Human-interpretable match scores that estimate false match likelihood
- Portable between client and server hardware and OS, and database platforms
- Support for all major image formats
- Enhanced functionality with optional Aware image preprocessing and QA SDKs
- C, .NET, JNI, and Web Service interfaces
- Support for 32-bit and 64-bit Windows and Linux

API FUNCTIONALITY

BIOMETRIC ENROLLMENT

- Subject add, update, and delete
- Automatic unique subject ID generation
- Accept preprocessed image/metadata objects from other Aware SDKs

BIOMETRIC SEARCH AND MATCH

- Match score from 1:1 comparison between two subjects or probe and selected subject
- Match score(s) from 1:many comparison between probe and full gallery

SEARCH AND MATCH CONFIGURATION

Tools for performance optimization based on:

- Database size/quality
- RAM/CPU
- Target speed/accuracy

Nexa|Fingerprint™

The Nexa|Fingerprint SDK provides high-performance algorithms for multistage fingerprint search or rapid, high-volume authentications. With recently optimized algorithms, the performance is comparable to other leading fingerprint search software products.

- **Multi-stage fingerprint matching algorithms**
- **Flats, rolls, and multi-finger images**
- **One through ten fingerprints and 14-image sets**
- **1:1 match, 1:many search, deduplication**
- **Human-interpretable match and confidence scores**

ENHANCED FEATURES WITH FASTCAPTURE, LIVESCAN API AND SEQUENCECHECK SDKS

- **Sequence checking**
- **High-performance segmentation**
- **ANSI/NIST ITL-1 2011 transaction parsing**
- **Quality scoring**
- **Live scan support**

Nexa|Face™

Nexa|Face is a high-performance facial matching and searching algorithm that can be trained on any database to optimize its matching performance.

- **1:1 match, 1:many search, deduplication**
- **Human-interpretable match and confidence scores**
- **Custom-trainable**

ENHANCED FEATURES WITH PREFACE™ SDK

- **Portrait normalization (tilt, scale, crop, brightness, contrast)**
- **Quality and compliance assurance**
- **Age, sex, and race estimation**
- **Facial features and attributes**
- **Configurable face finding**
- **Video input support**
- **Camera support**

Nexa|Iris™

Nexa|Iris is a high-performance iris matching and searching algorithm that

- **Search and match using one or two irises**
- **1:1 match, 1:many search, deduplication**
- **Human-interpretable match and confidence scores**

ENHANCED FEATURES WITH IRISCHECK™ SDK

- **Segmentation configuration**
- **ISO/IEC 29794-6 quality scoring**
- **Support for all NIST KIND formats**

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'sQualityCheck™ 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.

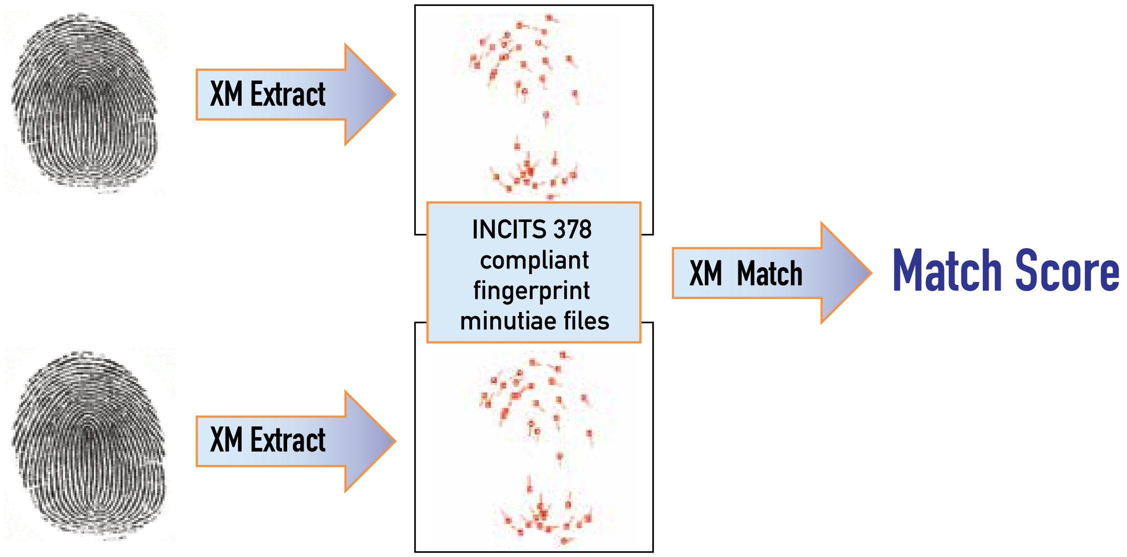
Because AwareXM is MINEX-certified, it is interoperable with template extraction and matching algorithms from many other vendors. This means that fingerprint templates generated and stored on a card using AwareXM can be biometrically verified by any other MINEX-certified matcher. Conversely, AwareXM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

AwareXM is also available in a version that is not MINEX-certified but achieves better matching performance when the AwareXM extraction and matching are paired.

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

FEATURES & 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
- Includes example programs with source



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.

©2015 Aware, Inc. www.aware.com

LiveScan API

Fingerprint Autocapture, Quality Assurance, and Scanner Abstraction

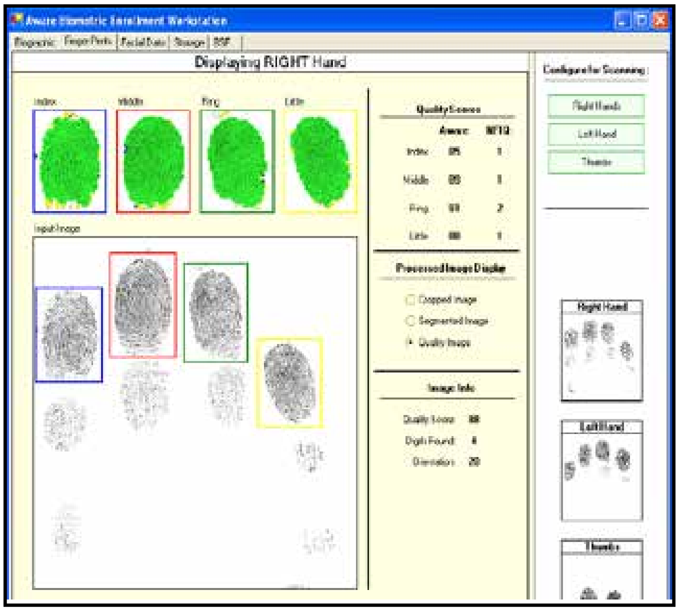
LiveScan API is an SDK that provides fingerprint capture device abstraction though a common API. It supports approximately forty single finger, multi-finger and palm capture devices and is designed to allow an application to support any of these devices with no changes to the application code. It is ideal for 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.

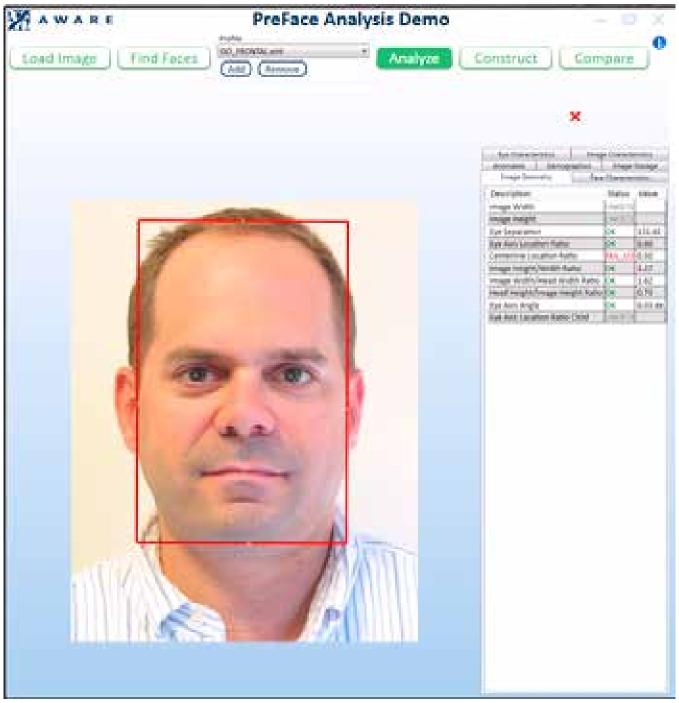
LiveScan API is included in the CaptureSuite SDK for full fingerprint capture and formatting.

PreFace™

Biometric Facial Image Autocapture, Quality Assurance, 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 enrolment 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. 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 and non-compliant features. 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.



Description	Status	Value
Image Width	[illegible]	
Image Height	[illegible]	
Eye Separation	OK	[illegible]
Eye Axis Location Ratio	OK	[illegible]
Centerline Location Ratio	FAIL	[illegible]
Image Height/Width Ratio	OK	[illegible]
Image Width/Head Width Ratio	OK	[illegible]
Head Height/Image Height Ratio	OK	[illegible]
Eye Axis Angle	OK	[illegible]
Eye Axis Location Ratio (Chin)	[illegible]	

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
- 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

PreFace functionality includes:

Face Characteristics

- Pose Angle Yaw
- Dynamic Range
- Brightness
- Saturation
- Smilee

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
- Background Color
  - Red
  - Green
  - Blue
- Background HSL
  - Hue
  - Saturation
  - Lightness
- Background HSV
  - Hue
  - Saturation
  - Value

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

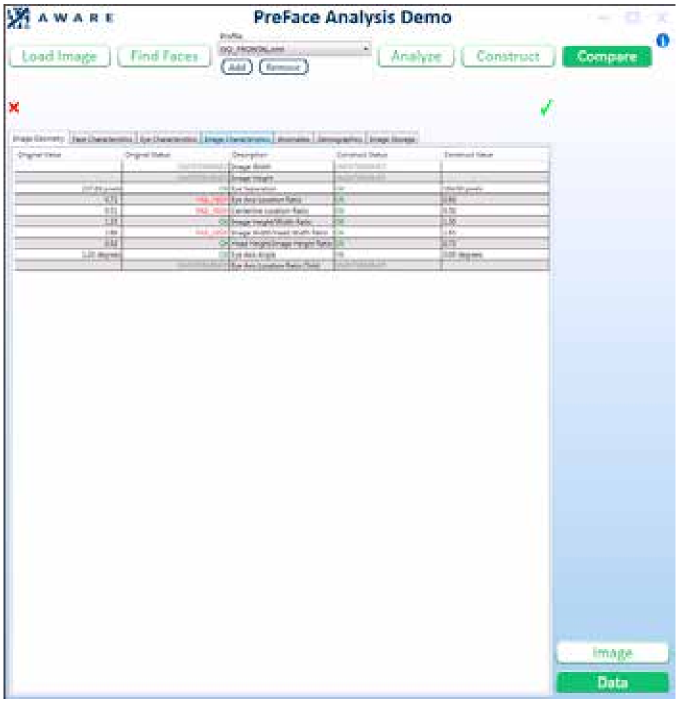
- Image Width
- Image Height
- Eye Separation
- Eye Axis Location Ratio
- Centerline Location Ratio
- Image Height/Width Ratio
- Image Width/Head Width Ratio
- Head Height/Image Height Ratio
- Eye Axis Angle
- Eye Axis Location Ratio (Child)

Demographics

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

Image Storage

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



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, and can be found on the GSA Approved Products List. An up-to-date list of cameras supported by Camera API is available from Aware upon request.

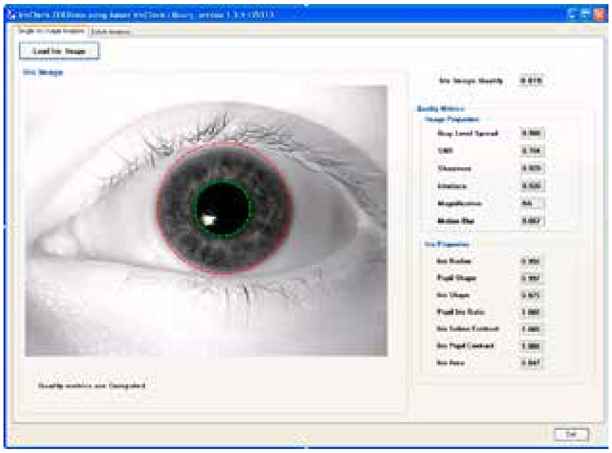
IrisCheck™

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 enrolment 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
- Degree of specularity



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
- Shadow detection

SDK FEATURES

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

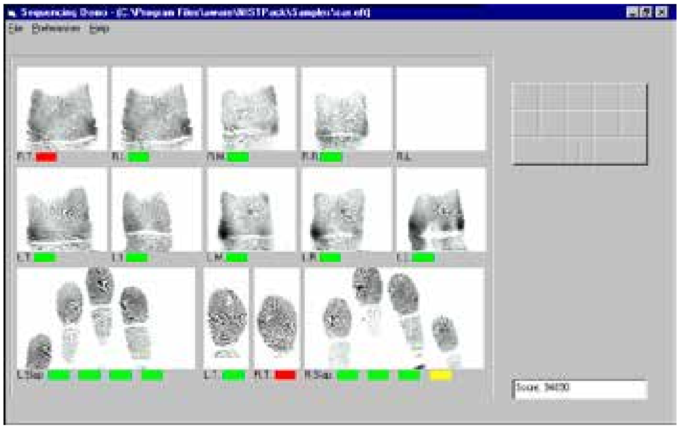
IrisCam API

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 enrolment 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.

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.



*Output of a SequenceCheck example program that operates on a tenprint card. Colors designate a **match**, **no match**, or **match pending**. For each two finger match attempt a score is returned. A match/no-match threshold can be set through the "preferences" pull-down menu.*

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.

FINGERPRINT MATCHING

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 full hand “handedness” detection (left/right?), 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.

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 1-2011 (and earlier) compliant data formatting. AccuPrint can be used to generate high quality, FBI-certified printouts of fingerprint images or entire tenprint cards.

SequenceCheck is included in the CaptureSuite product along with FastCapture and NISTPack for a comprehensive fingerprint capture solution.

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

QualityCheck™

Fingerprint Image Quality Analysis and Scoring Software

QualityCheck is an advanced fingerprint image quality scoring software library included in Sequence-Check and Aware WSQ1000 SDKs. QualityCheck uses advanced algorithms to assess whether a fingerprint image is of sufficient quality for biometric matching. QualityCheck implements a specific measure of finger image quality that is based on the continuity of ridge flow across all regions of a finger image, and returns information based on the following factors:

1. **Image smudges due to movement, improper finger placement, or excess moisture**
2. **Image darkness due to excess pressure**
3. **Image lightness due to inadequate pressure**
4. **Mis-calibrated sensor**
5. **Small image**
6. **Missing core or delta**
7. **Relative quality as compared to other images**

Quality Scoring

QualityCheck generates an overall score between 0 and 100, and provides information on areas of the image that exhibit problems. These areas are returned to a software application as arrays of pixel regions or as a color-coded image of the finger, which indicates the specific problems with the finger image. This functionality can improve the ability of an operator to screen bad images.

FEATURES & FUNCTIONALITY

- Includes C callable library or ActiveX control designed to be integrated into a larger application
- Includes source code to example programs
- Provides a score indicating quality of finger ridge data
- Manual and auto image cropping functions to remove the finger ridge data from a noisy or large background image
- Provides minutiae counts and number of core/delta found
- Indicates pixel regions that are good, too dark, too light, or that have smudged/broken finger ridges
- Color-coded image-based function returns this same information
- Usable with all matchers and systems
- Statistically reliable results
- Supported by Microsoft Windows, Linux, and Solaris platforms
- Fully featured C Language API
- C#/.NET wrappers
- Example programs with source
- Java Native Interface support
- Microsoft Windows and Linux Support

The finger images shown below, in order from best to worst quality, are samples from field deployed systems. The quality values and color coding information are returned by the Aware QualityCheck functions. The color codes provide quick visual assistance to identify the following gross problems with an image:

Blue	**smudged or broken areas**
Red	**areas that are too dark**
Yellow	**areas that are too light**
Green	**areas of good quality**

Typical Classification Thresholds

85-100 Good
75-84 Adequate
60-74 Marginal
0-59 Poor

QUALITY SCORE DISTRIBUTION

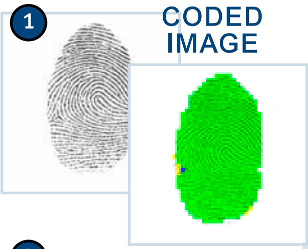
The correlation between the scores and the general quality of an image can be understood by examining the distribution curve shown in the graph below. Each of 17,000 FBI-compliant live-scanned images (different scanners, impressions, and rolls) are scored and plotted.

MINUTIAE AND CORE/DELTA

QualityCheck helps identify partial images or images consisting only of fingertips. Image #7 shows an example where the minutiae count is low, and no core or delta was found. Partial finger images can pose a particular problem because they may have good ridge flow, but still do not provide the correct information. Lack of core/delta and low minutiae counts helps to flag those images.

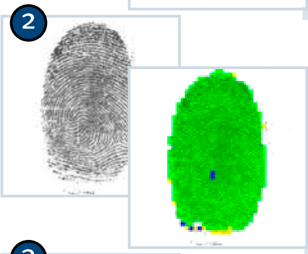
ORIGINAL IMAGE **COLOR-CODED IMAGE** **QUALITY VALUES**

1



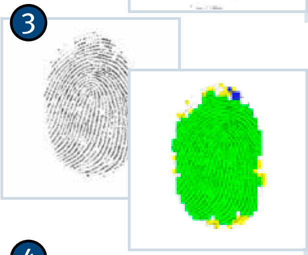
Quality Score	91
Minutiae	46
Core/delta Found	Yes
# Good Pixels	82.5K
# Bad Pixels	1K
Q Percentile	99%

2



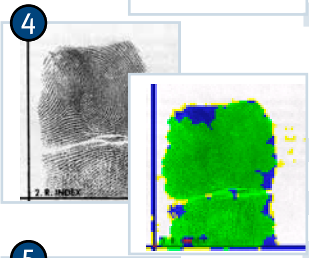
Quality Score	83
Minutiae	78
Core/delta Found	Yes
# Good Pixels	100K
# Bad Pixels	2.6K
Q Percentile	68%

3



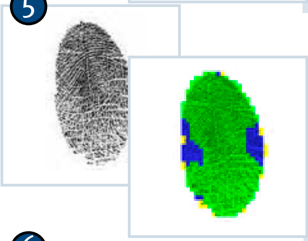
Quality Score	78
Minutiae	29
Core/delta Found	Yes
# Good Pixels	72.5K
# Bad Pixels	5.4K
Q Percentile	44%

4



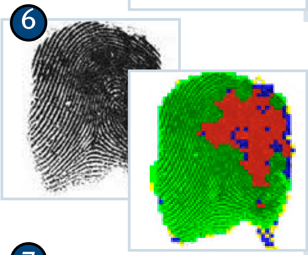
Quality Score	50
Minutiae	139
Core/delta Found	Yes
# Good Pixels	266K
# Bad Pixels	80.6K
Q Percentile	3%

5



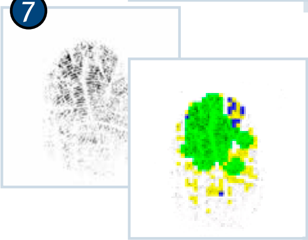
Quality Score	41
Minutiae	108
Core/delta Found	Yes
# Good Pixels	64K
# Bad Pixels	11.3K
Q Percentile	1%

6



Quality Score	31
Minutiae	95
Core/delta Found	Yes
# Good Pixels	86.2K
# Bad Pixels	59.9K
Q Percentile	<1%

7



Quality Score	24
Minutiae	8
Core/delta Found	No
# Good Pixels	26.9K
# Bad Pixels	14.8K
Q Percentile	<1%

NUMBER OF GOOD PIXELS

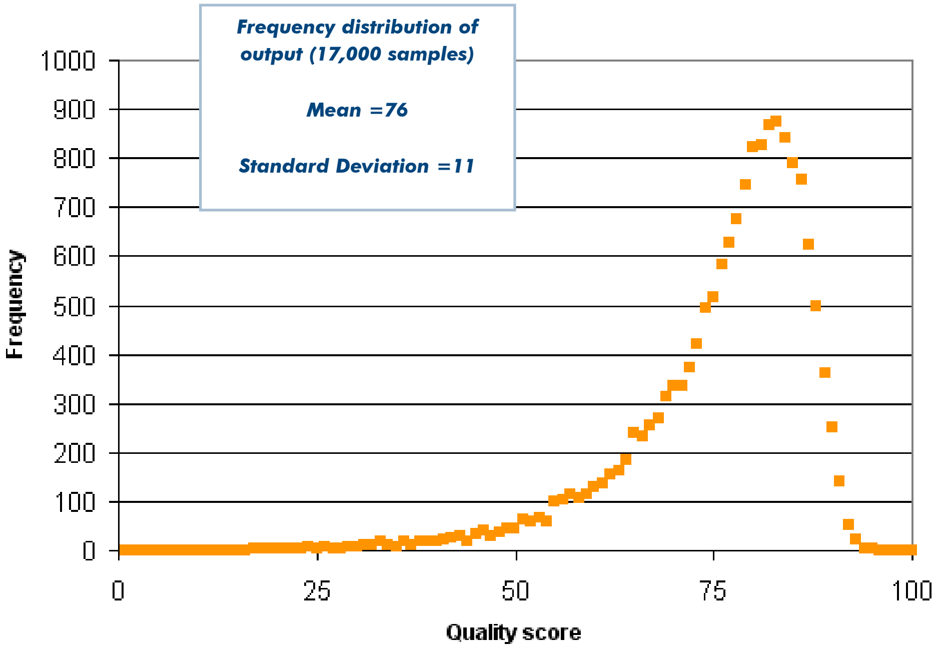
Provides the total count of the green area for each image. This is the part of the image where Minutiae points likely can be extracted from. This number can be used to flag images that are too small.

NUMBER OF BAD PIXELS

Provides the total count of the red (too dark), yellow (too light) and blue (broken, smudged) pixels. Images with low ratios of good-to-bad pixels (images #4, 5, 6, and 7) closely correlate with low quality scores.

Q PERCENTILE

Describes where the given image falls in the sample distribution shown in the plot below. The value indicates the percent of images from this database of 17,000 FBI-compliant scanned fingers that exhibited lower scores.

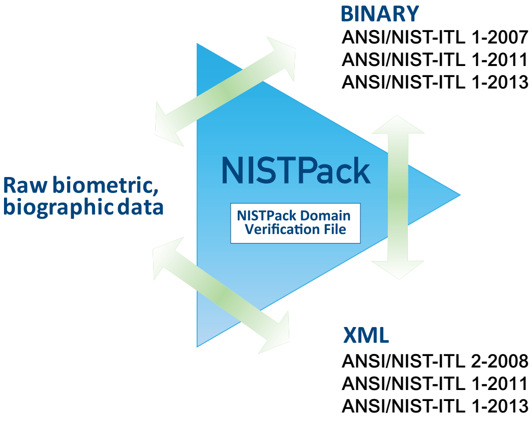


Frequency distribution of quality score results

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.

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
- 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

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.

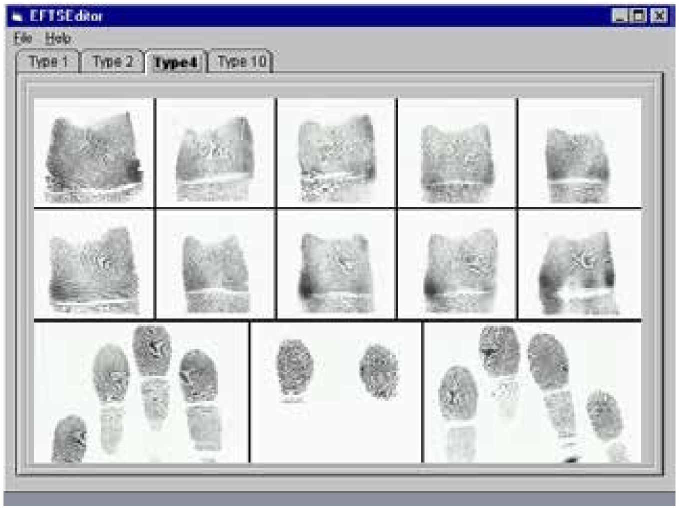
Editing of transaction files. This entails making changes to existing files or correcting items and assuring that the new file is compliant.

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.

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)**
- **facial, scar/mark, and tattoo data (Type-10 Record)**
- **latent images (Type-13 records)**
- **variable resolution (500 and 1000 ppi) finger images & 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)**
- **iris images (Type-17 Record)**

Other biometric data not handled by the other records (Type-99 Record)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 & validation of most of the global agency-specific implementations (domains) of the standard defined. This includes:



Display of Type-4 records in transaction editing tool

- **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**

ANSI/NIST-ITL 1-2011 will add substantial improvements and the following new record types:

- **expanded Type-9 minutiae record that supports latent image extended feature sets (EFS)**
- **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)**

ICAOPack

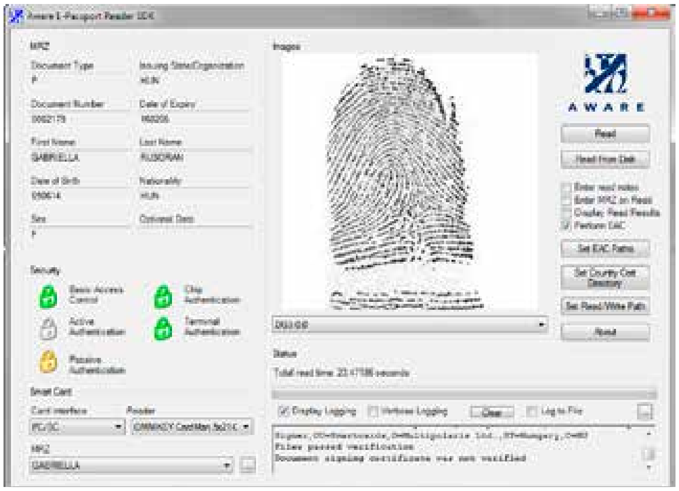
Data Reading, Personalization, and Authentication for E-Passport Solutions in accordance with ICAO Doc 9303

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.



MRZ

Document Type: P
Issuing State/Organization: HUN
Document Number: 0002179
Date of Expiry: 160206
First Name: GABRIELLA
Last Name: RUSORAN
Date of Birth: 050614
Nationality: HUN
Sex: F
Optional Data:

Security

Basic Access Control
Chip Authentication
Active Authentication
Terminal Authentication
Passive Authentication

Smart Card

Card interface: PC/SC
Reader: OMNIKEY CardMan 5x21 C
MRZ: GABRIELLA

DG3 00

Status

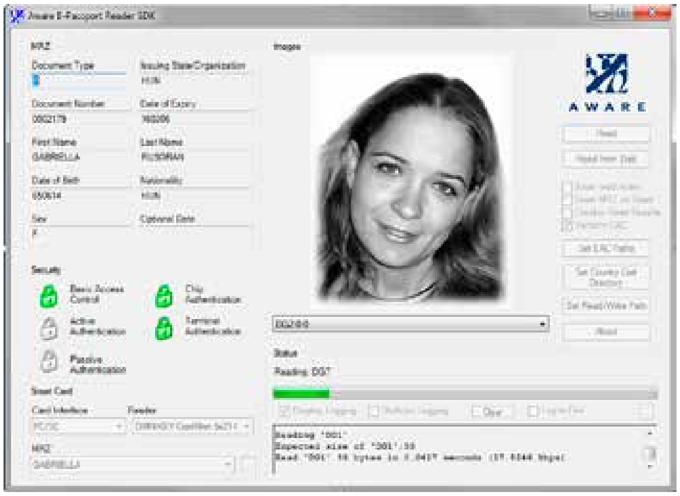
Total read time: 23.41786 seconds

```
Signer, CO=[illegible], O=[illegible] Ltd., ST=Hungary, C=HU
Files passed verification
Document signing certificate was not verified
```

Reading of a data groups from an e-passport and display of "DG3" fingerprint image

FEATURES & FUNCTIONALITY

- Software development kit includes example programs and documentation
- Easy to use and understand
- Programmable in C, C++, .NET, and Java
- 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
- Fully featured C Language API
- C#/.NET wrappers
- Example programs with source
- Java Native Interface support
- Microsoft Windows and Linux Support



MRZ

Document Type

Issuing State/Organization: HUN

Document Number: 0002179

Date of Expiry: 160206

First Name: GABRIELLA

Last Name: FILSORAN

Date of Birth: 650614

Nationality: HUN

Sex: F

Optional Data

Security: Basic Access Control, Chip Authentication, Active Authentication, Terminal Authentication, Passive Authentication

Smart Card

Card Interface: PC/SC

Reader

MRZ: GABRIELLA

Images: DG2:0:0

Status: Reading DG7

```
Reading 'DG1'
Expected size of 'DG1':93
Read 'DG1' 93 bytes in 0.0417 seconds (17.9344 kbps)
```

Reading of a data groups from an e-passport and display of "DG2" facial image.

Other Aware Products for E-Passports

ICAOPack can be used seamlessly with other Aware software products:

- **PreFace for autocapture and compliance assurance of facial images and abstraction of cameras**
- **FastCapture with Live Scan API for automated ten-print capture using a live scan device**
- **NISTPack to generate standards-compliant biometric transactions**
- **AwareXM to generate MINEX-certified finger templates from finger images**
- **Biometric Service Platform (BioSP) to centrally administrate workflow and transport and storage of enrollment data**

ICAOPack is included in Aware's ICAOSuite family of SDKs.

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.

The PIVPack SDK is designed upon Aware's experience building software tools to support other biometric data interchange standards, several of which form the basis of FIPS 201 and its companion biometric standards. (See NISTPack, ICAOPack, M1Pack).

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.

FEATURES & FUNCTIONALITY

- Software development kit includes example programs and documentation
- Easy to use and understand
- Programmable in C, C++, .NET, and Java
- 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
- Fully featured C Language API
- C#/.NET wrappers
- Example programs with source
- Java Native Interface support
- Microsoft Windows and Linux Support

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.

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**

The SDK includes example programs with source code that are useful as a guide to proper usage and integration into a larger system. Also included are FBI-certified WSQ, JPEG, and JPEG 2000 for compression and decompression of fingerprint and facial images. Aware's JPEG 2000 implementation includes region of interest (ROI) compression as recommended in SP 800-76 for optional storage of facial images on ID card memory.

Other Aware Products for PIV

PIVPack can be used seamlessly with other Aware software components:

- **PreFace, used to analyze and optimize facial images and assure their compliance with ANSI/INCITS 385**
- **FastCapture with Live Scan API for automated tenprint capture using a live scan device**
- **NISTPack to generate standards-compliant biometric transactions**
- **AwareXM to generate MINEX-certified finger templates from finger images**
- **Biometric Services Platform (BioSP) to centrally administrate workflow and transport and storage of enrollment data**

PIVPack is included in Aware's PIVSuite™ family of SDKs.

Aware WSQ1000

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.

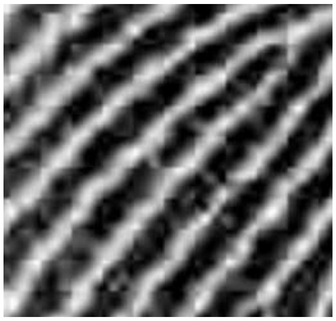
Today, most of the world's large, high throughput, fingerprint management and matching systems depend on Aware WSQ1000 to manage the compression and decompression of finger and palm image data. All finger and palm images submitted to the FBI are managed by Aware WSQ1000.

Aware WSQ1000 is the choice of most large state and federal systems because of its:

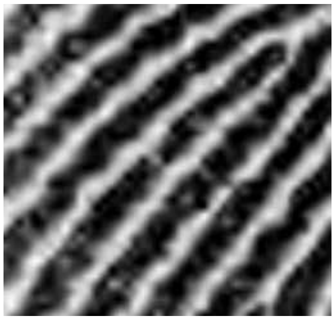
- **Runtime performance.** Aware WSQ1000 is 4-5 times faster than most other WSQ implementations that share a common code base
- **Error resilience**. Aware WSQ1000 has been exposed to and processed more images than any other implementation of the standard. It will not crash or bring a system down when 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
- **Continuous compliance certification with the FBI**. 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.

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)
- 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
  - Apple iOS
  - Blackberry Java

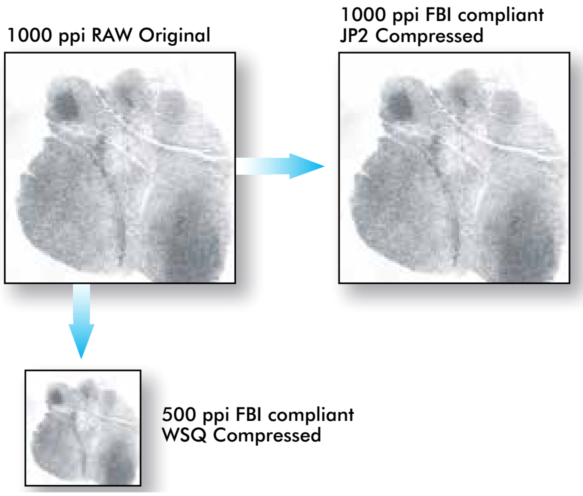


Section of a digital fingerprint image that has been compressed 15:1 with the JPEG algorithm. Note the block artifact that is inherent in the algorithm. The image has been zoomed by 4.

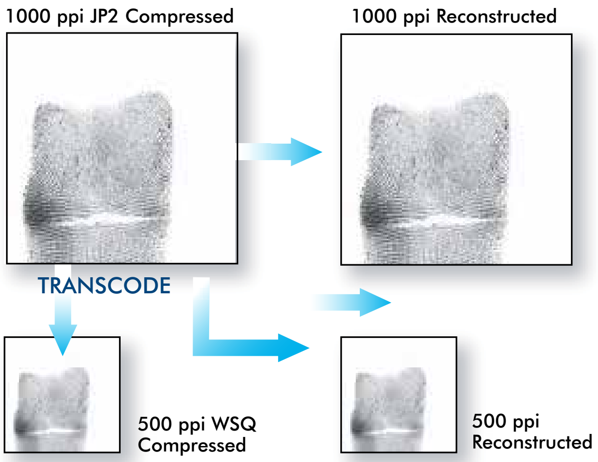


Section of the same fingerprint image that has been compressed 15:1 with the WSQ algorithm. Note the absence of the block artifact. The image has been zoomed by 4

COMPRESSION


1000 ppi RAW Original
1000 ppi FBI compliant JP2 Compressed
500 ppi FBI compliant WSQ Compressed

DECOMPRESSION



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.

Aware JPEG 2000

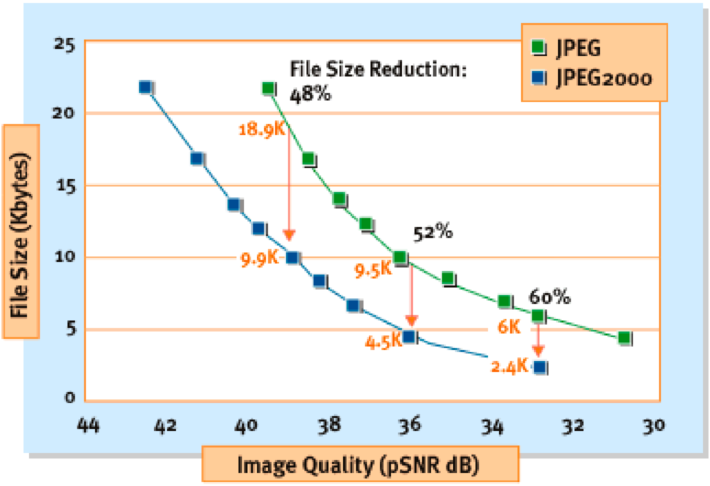
For Compression and Decompression of Biometric Face and Iris Images

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).

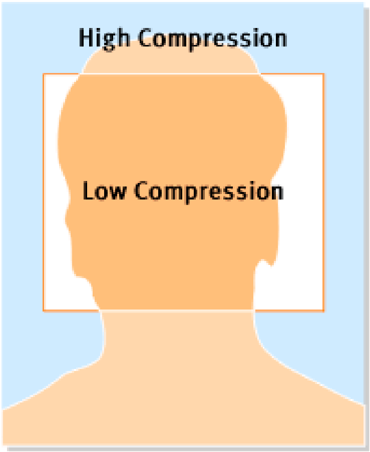
Aware's JPEG 2000 compression libraries are available as a standalone SDK or as part of several other Aware SDK products.

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

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 administrate 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.

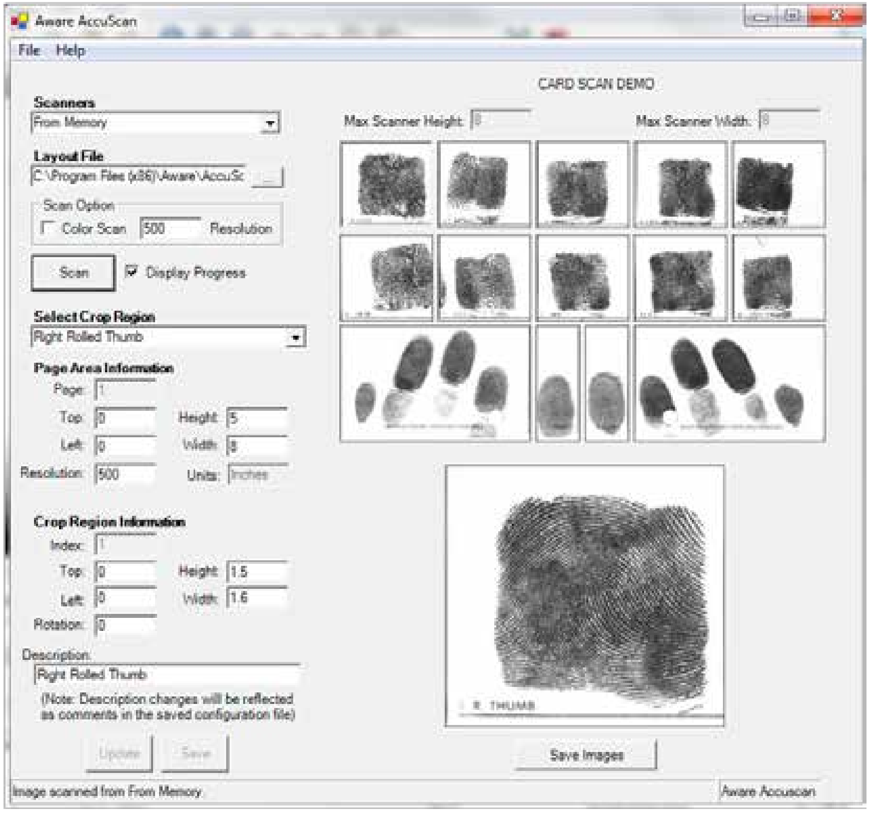
The combined NISTPack/AccuScan software toolset provide the following:

- **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



Scanners: From Memory

Layout File: C:\Program Files (x86)\Aware\AccuSc

Scan Option: ☐ Color Scan 500 Resolution

☑ Display Progress

Max Scanner Height: 8 Max Scanner Width: 8

Select Crop Region: Right Rolled Thumb

Page Area Information
Page: 1
Top: 0 Height: 5
Left: 0 Width: 8
Resolution: 500 Units: Inches

Crop Region Information
Index: 1
Top: 0 Height: 1.5
Left: 0 Width: 1.6
Rotation: 0

Description: Right Rolled Thumb

(Note: Description changes will be reflected as comments in the saved configuration file)

Image scanned from From Memory

Aware Accuscan

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.

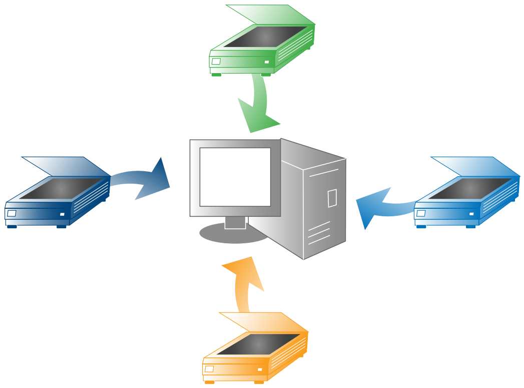
AccuScan manages this problem through an XML-based configuration file that holds the layout details of the original paper document. This file describes the size and location of each fingerprint or palm print image. AccuScan includes a utility (executable and source) that enables the easy creation of 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'sFormScanner applications for fingerprint card and form scanning.

AccuScanMB

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.

When used with NISTPack, a solution is able to seamlessly create or read ANSI/NIST fingerprint transactions and then print high-quality images.

ACCUPRINT AS A STAND-ALONE LIBRARY

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.

GENERATING TENPRINT CARD GRAPHICS

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

1. Text-based layout files

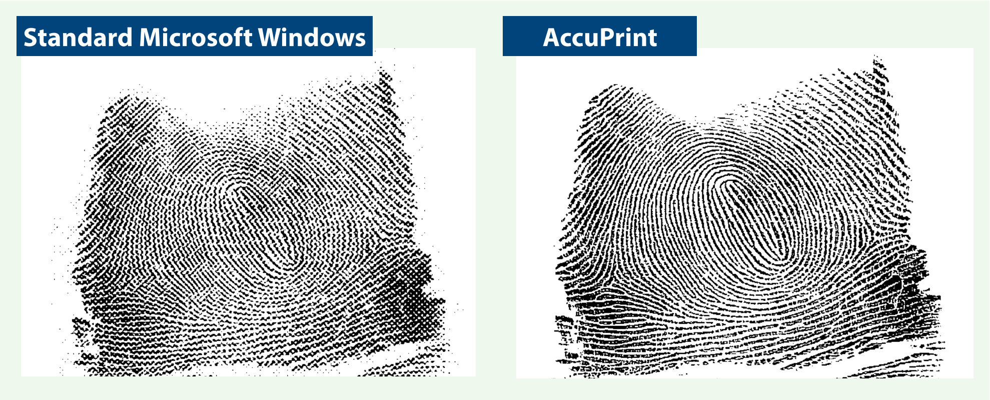
These files use a simple suite of line and text drawing commands to draw every line and text segment present on the card. The files also allow the use of graphical images and icons.

2. Scanned image of a blank card

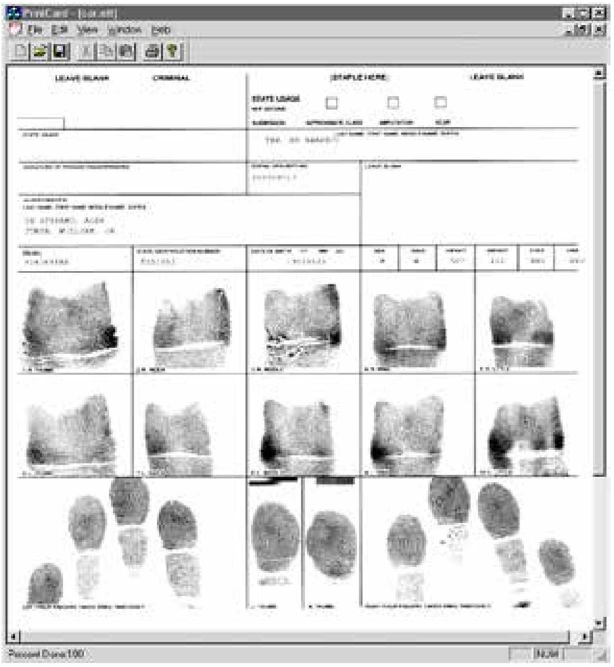
A blank tenprint card scanned and saved as a TIF or JPEG image can also be used by AccuPrint to regenerate tenprint card graphics. This method is particularly useful for cards with complicated graphics, fonts, or character sets.

FEATURES & 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
- Includes documentation and example programs for ease of use
- Meets the FBI Image Quality Specification (IQS) for printers
- C language API for software developers
- ActiveX control for Visual Basic programming
- Includes runtime applications and demos with source code



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.



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.

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.

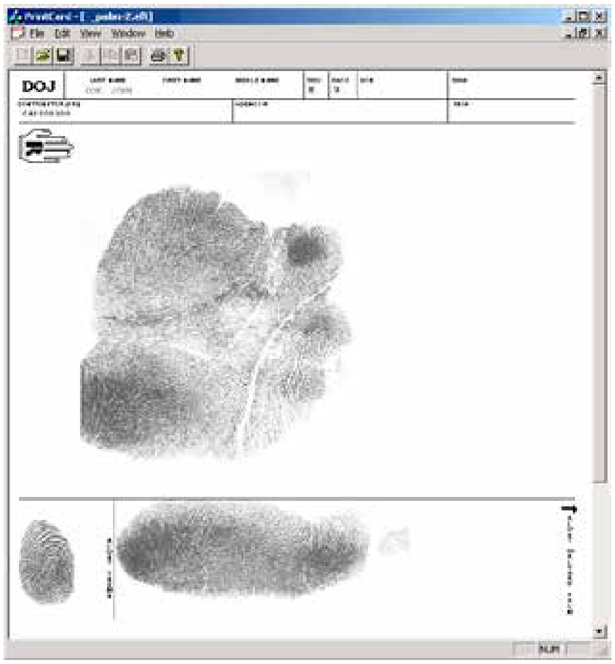
BARCODE PRINTING

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 check boxes based on the contents of a demographic data field**



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.

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.

Smart Phones and Tablets

PreFace™ Mobile

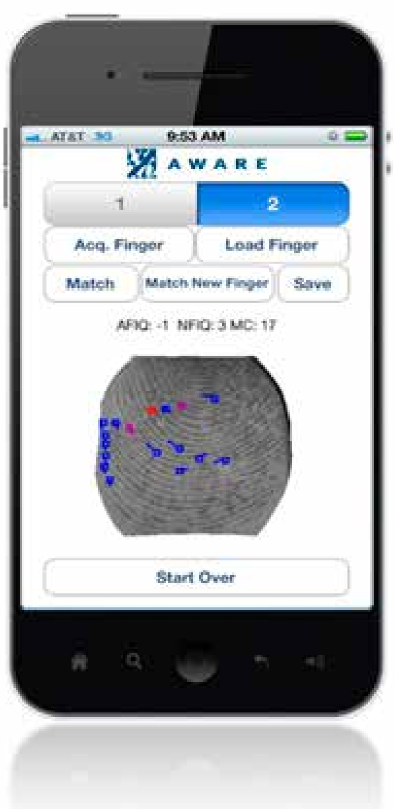
BIOMETRIC FACIAL IMAGE AUTOCAPTURE AND QUALITY/COMPLIANCE ASSURANCE ON MOBILE DEVICES

PreFace Mobile is an implementation of PreFace optimized for mobile applications running on Android, iOS, Blackberry, and Windows Phone operating systems. PreFace Mobile performs facial image capture using the smart phone camera and like PreFace, performs automatic "tilt, scale, and crop" processing to optimize the image and analysis to assess the quality and standards-compliance.

Aware WSQ 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, iOS, Blackberry, and Windows Phone operating systems. Aware WSQ Mobile provides high-performance, FBI-certified implementation of the WSQ compression algorithm for fingerprint images on mobile devices.



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, iOS, Blackberry, and Windows Phone 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 1-2011 (and earlier).

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 wish 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 tenprint files or for any other type of transaction.

- **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.

- **EDITING OF TRANSACTION FILES**
  This entails making changes to existing files or correcting items and assuring that the new file is compliant.

PIVPack™ Mobile

READING AND AUTHENTICATION OF PIV CARDS ON MOBILE DEVICES

PIVPack Mobile is an implementation of PIVPack designed to operate on mobile devices running Android, iOS, Blackberry, and Windows Phone operating systems. It performs JPEG/JPEG 2000 image decompression and parsing of PIV card data groups including biographic data, face images, and fingerprint templates. It parses security objects and performs authentication as required in compliance with FIPS 201 standards.

PIVPack Mobile includes a command line reference application as well as user interface applications for specific hardware devices. It can also interoperate with BioSP to perform centralized biometric authentication, event logging, and other functions.

ICAOPack Mobile

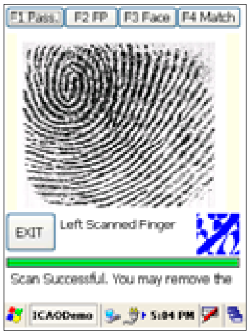
READING AND AUTHENTICATION OF E-PASSPORTS ON MOBILE DEVICES

ICAOPack Mobile is an implementation of ICAOPack designed to operate on mobile devices running Android, iOS, Blackberry, and Windows Phone operating systems. It performs decompression of WSQ fingerprint images, JPEG 2000 facial images, and parsing and display of ICAO-compliant LDS data groups including MRZ data. It parses all security objects and performs passive and active authentication and basic and extended access control (BAC and EAC) as required in compliance with the ICAO Doc 9303 standards.

ICAOPack Mobile includes libraries and a command line reference application as well as user interface applications for specific hardware devices. It can also interoperate with BioSP to perform centralized biometric authentication, event logging, and other functions.

AwareXM™ Mobile

MINEX-CERTIFIED FINGERPRINT TEMPLATE EXTRACTION AND MATCHING ON MOBILE DEVICES



Scan Successful. You may remove the

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, Blackberry, 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.

CaptureSuite™

Automated Capture, Analysis, and Processing of Fingerprints

Aware's CaptureSuite is a bundle of software development kits (SDK) supporting the development of applications with comprehensive functionality for capture of either live scan or card scan fingerprint images. CaptureSuite provides several quality and compliance assurance mechanisms for a variety of applications, as described below. CaptureSuite includes the following Aware SDKs:

LIVE SCAN

CARD SCAN

SequenceCheck

- Fingerprint segmentation and sequence checking

NISTPack

- FBI-certified WSQ fingerprint image compression
- ANSI/NIST-ITL 1-2011 (and earlier) file formatting and validation

LiveScan API

- Real-time image segmentation and bounding
- Real-time quality scoring
- Real-time left/right hand identification
- Real-time angle measurement
- Real-time detection of finger on edge

OR

AccuScan

- Fingerprint card segmentation
- Fingerprint image quality scoring

Inquire|Search™

Text-Based Filter, Search, and Match

Inquire|Search™ 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|Search is optimized for processing and analysis of data that includes biometrics.

Inquire|Search provides many advanced text matching comparison algorithms and flexibility in how matching algorithms behave (e.g. thresholds, data definitions). Inquire|Search is fully scalable, with infrastructure that automatically determines processing resources and optimizes their utilization.

FUZZY NAME AND ADDRESS MATCHING

Inquire|Search 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.

FUNCTIONALITY

- Probabilistic (fuzzy) text search, and match
- Name and address matching
- Biometric search pre-filtering
- Soft biometrics

APPLICATIONS

- Data quality analysis and repair
- Identity record matching
- Biometric search pre/post-filtering
- Know your customer/visitor
- Visa/asylum fraud detection
- Bank/insurance fraud detection

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

NAME VARIANTS

Brian ≈ Bryan
Sara ≈ Sarah

NICKNAMES

Jack ≈ John
Bobby ≈ Robert

SPECIAL CHARACTERS

Mueller ≈ Müller
OCallahan ≈ O'Callahan

PHONETIC SIMILARITIES

Mohamed ≈ Muhammad
Geoffrey ≈ Jeffrey

TYPOS

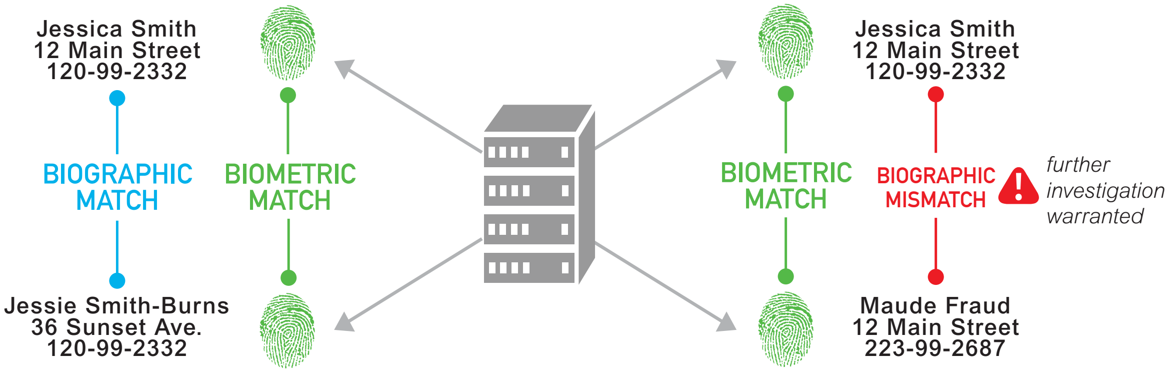
Washington ≈ Washimgton

MISSPELLINGS

Albuquerque ≈ Albequrque

NAME CHANGES

Laura Smith ≈ Laura Smith-Jones



BIOGRAPHIC DATA MATCHING

Inquire|Search 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.

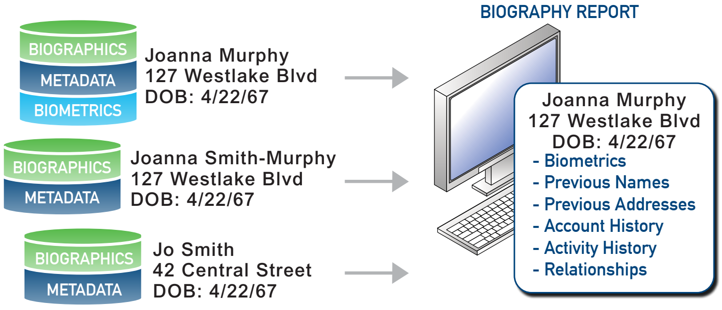
Inquire|Resolve™

Data integration, Identity resolution, and Relationship Detection

Inquire|Resolve is an SDK that 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.

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|Resolve 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, nonmatches, and crosslinks.



FUNCTIONALITY

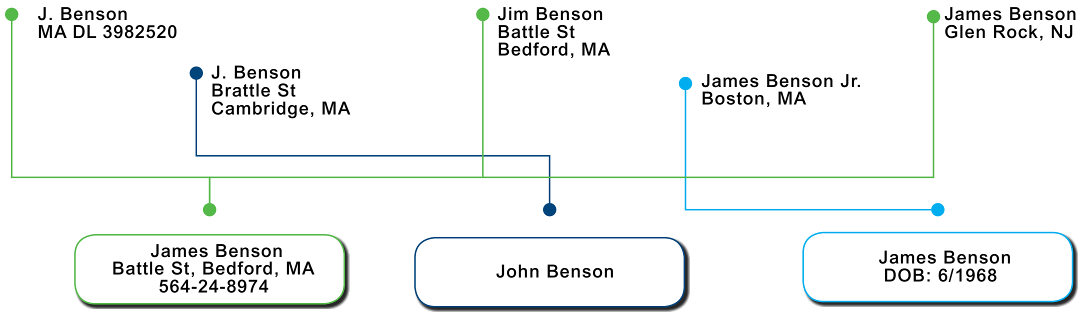
- Identity data analysis
- Identity data cleanup and QA
- Data integration and identity resolution
- Link analysis for relationship discovery

APPLICATIONS

- Data quality analysis and repair
- Identity record matching
- Biometric search pre/post-filtering
- Know your customer/visitor
- Visa/asylum fraud detection
- Bank/insurance fraud detection

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



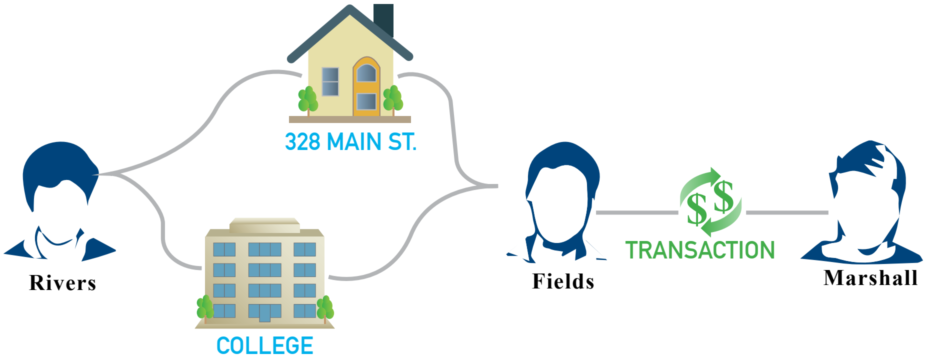
DATA INTEGRATION AND IDENTITY RESOLUTION

Inquire performs integration of identity data records across databases, linking attributes and encounters associated with a particular individual to a single identity record. Inquire|Resolve 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|Resolve 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


328 MAIN ST.
Rivers
COLLEGE
Fields
TRANSACTION
Marshall