



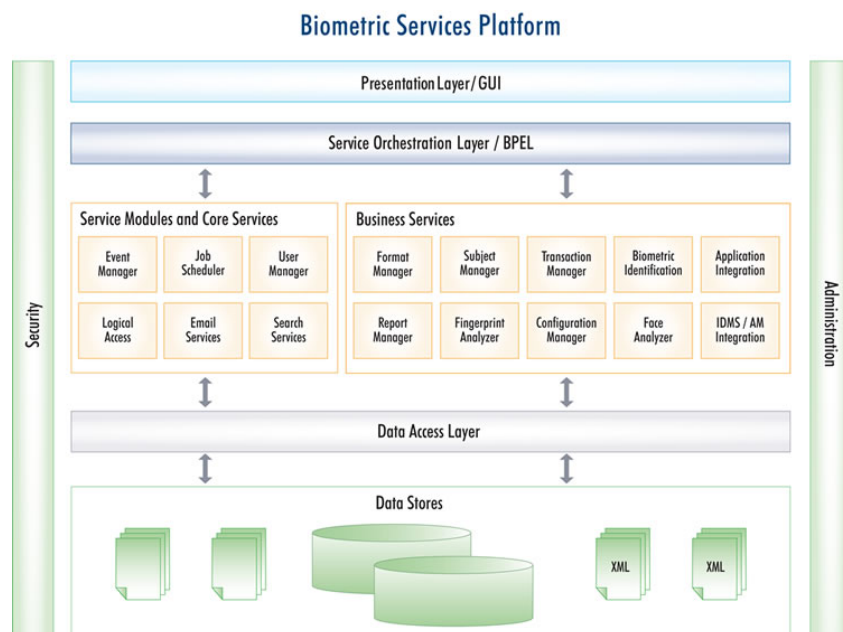
Rogue DNA Forensic Lab Biometric Application Server

Rogue DNA's Forensic Lab suite (RFL) provides the following functions. Data can be seamlessly exchanged between each module:

- Face recognition & partial face recognition
- Fingerprint recognition and compliance with biometric standards
- Fingerprints & facial images – conversion of paper prints to electronic
- Biometric Application Server
- Document authentication

Biometric Application Server

Rogue DNA's Biometric Services Platform (BioSP) is a modular, configurable, service-oriented application server platform used to integrate advanced biometric data processing and management functionality into an enterprise solution. BioSP is well suited for applications that require the collection of biometrics throughout a distributed network, and subsequent



aggregation, analysis, processing, distribution, authentication, and sharing of this data with other system components. BioSP manages all aspects of transaction workflow, including

messaging, submissions, responses, and logging. BioSP incorporates the latest open-source components and is J2EE-compliant.

BioSP is differentiated not only by its high degree of modularity and configurability, but also by its advanced biometric capabilities. BioSP performs biometric authentication and duplicate checking, centralized image processing, data formatting and transcoding, and biometric image quality assurance and reporting.

BioSP also provides connectivity to endpoints used for biometric image and data capture, such as for enrollment, verification, and identification. BioSP establishes connectivity to back-end systems including internal and external AFIS/ABIS, as well as systems for identity management, card management, and credential personalization. BioSP can also manage configuration and distribution of client-based enrollment software.

Key Functionality

- Performs automated biometric image and data analysis, processing, formatting, quality assurance, and reporting
- Utilizes web services in support of a 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:N matching for verification, identification, and duplicate checking
- Enables centralized system administration and user management
- Enables advanced reporting capabilities for fast troubleshooting of capture problems
- Enables centralized configuration, distribution, and management of client software
- Supports fingerprint, face, palm, and iris modalities

Key Features and Benefits

- Provides a flexible, configurable design for quick adaptation to legacy systems and different customer requirements
- Reduces costs through simplification of software distribution, support, and maintenance
- Increases overall efficiency and reliability by providing a common, unified platform that addresses disparate customers and business processes
- Improves transaction success rates through data redundancy, guaranteed delivery, and automated quality analysis and reporting
- Reduces impact on central repositories by aggregating client connections and biometric transaction submissions and responses
- Reduces support costs by eliminating ambiguity as to the status of submitted transactions, providing assurance and guidance to workstation operators
- Improves data and transaction security by enabling secure communications, digital signatures, and encryption of data at rest
- Increases visibility and control over solutions through centralization of complex processing tasks and administration