Biometric Solutions for Banking and Retail

Aware provides biometric solutions for employee- and customer-facing security and fraud prevention applications within the banking and retail arenas for biometric identity proofing and biometric authentication.

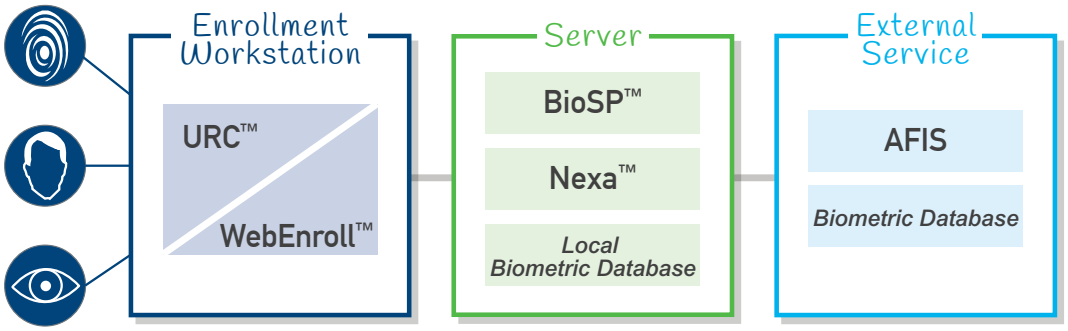
Biometrics can be used as an identity proofing tool towards "know your employee" or "know your customer" security efforts as part of an employee or customer onboarding process. Biometric authentication is used to secure access to sensitive financial data and transactions, including payments. These solutions can be also provided to third-party companies wishing to provide biometric identity proofing or biometric authentication as cloud-based services.

Identity proofing:

Know Your Employee/Customer

Aware software can be used to deploy biometrics identity proofing as a key element of "Know Your Employee (KYE)" or "Know Your Customer (KYC)" onboarding efforts. Applicants for employment or new customer accounts can be biometrically enrolled and searched in a biometric database to ensure that they are representing their identity honestly and consistently. In this way, identity proofing can prevent an individual from registering multiple identities in order to conceal information.

In Aware identity proofing solutions, BioComponents™ are used either within WebEnroll™ or URC™ to collect biometric images (fingerprint, face, and/or iris) from the applicant. The biometrics are submitted to BioSP running on a central server. Applicant records are stored securely in BioSP Subject Manager. A biometric search is performed by Nexa™ algorithms. BioSP Format Manager and Transaction Manager can be used to submit standards-compliant biometric records to the FBI or other external government systems for search.



Employee/customer authentication

Aware software can be used to deploy biometrics-enabled strong authentication of employees and customers. Authentication can be performed from either a client workstation or mobile device. Biometric template storage and matching can occur on the mobile device or alternatively on the server. Aware software supports different architectures and workflows depending on the level of security required and the nature of the application.

Match-on-server from client workstation (in-band).

Biometrics and enrolled and bound to identity information centrally. Biometric authentication takes place on a central server, with all biometric data stored securely on the server. A biometric match is required on the server to enable authentication. This solution might be used to grant access to information and assets to company employees. This architecture is analogous to using usernames and passwords to gain access to employer networks and data.

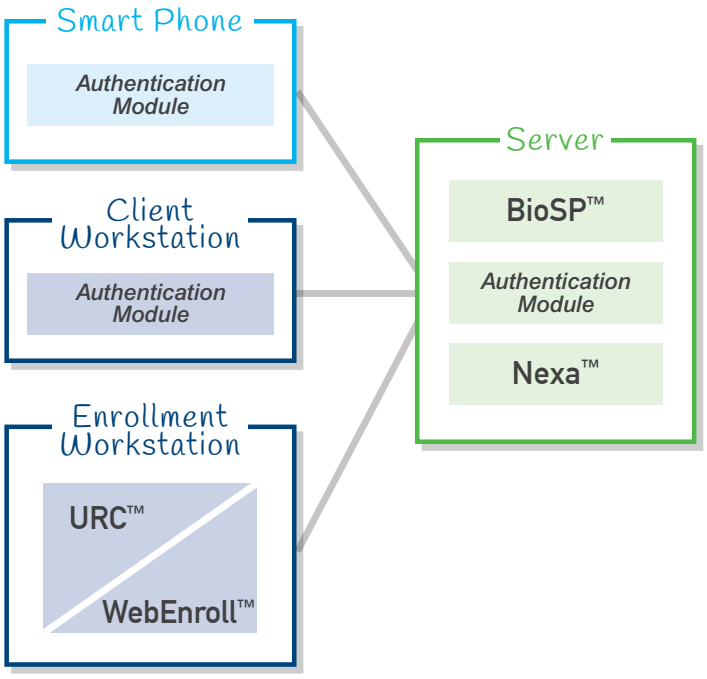
Match-on-server from point-of-sale (out-of-band).

Biometrics are enrolled and bound to identity data centrally. When identity authentication is required, such as part of a retail purchase, biometrics are collected and sent to a central server for authentication, with results reported back to the attendee at the point-of-sale. This is considered "out-of-band" because the biometric authentication is taking place in parallel with the purchase process, as opposed to a serial step within a single communication path.

For server-based authentication applications, enrollment is first performed. BioComponents are used either within WebEnroll or URC to enroll biometric images (fingerprint, face, and/or iris) from the applicant. The biometrics are submitted to BioSP running on a central server. Biometrics are stored securely in BioSP Subject Manager. A biometric match is performed by Nexa algorithms.

Match-on-device from mobile (in-band).

Biometric authentication takes place within an application running on a smart phone. A biometric match on the device is required to engage in a PKI challenge/response exchange with the server. The biometric reference is stored on the device and only PKI data is exchanged. Authentication can serve to secure access to financial information or transactions conducted from a smart phone. This architecture is analogous to use of a PIN on a smart phone. Open technical standards such as FIDO can be employed to define interfaces and protocols.



AWARE

781.276.4000 | sales@aware.com | www.aware.com

Aware is a leading global supplier of biometrics software products and solutions since 1993. We provide biometric enrolment SDKs, controls and applications, text and biometric search and match algorithms, and a biometric server platform. Our products are used to build biometric solutions for a variety of applications including law enforcement, border control, access control, credentialing, defense, and intelligence.