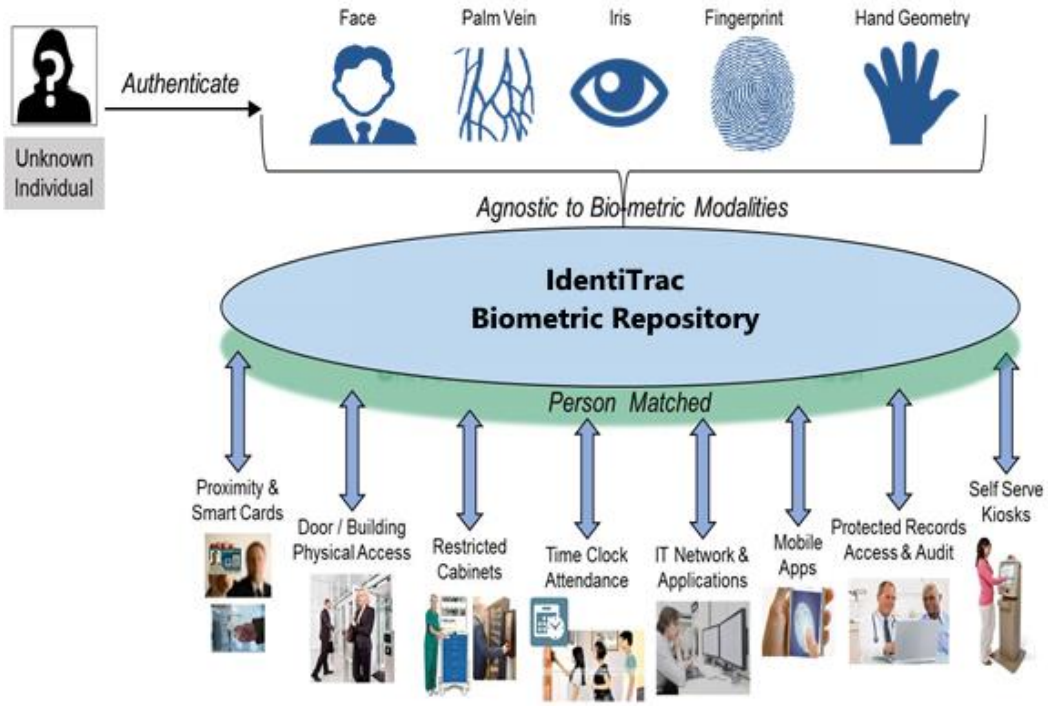
Securlinx Corporation
39555 Orchard Hill Place
Suite 600
Novi, MI 48375
Ph. 304.284.5020
securlinx.com

Trusted identity verification across the enterprise

With IdentiTrac®, Securlinx provides an enterprise-level, identity verification platform that manages all types of biometric identity data and is completely vendor agnostic as to scanning device, sensor hardware or the software used for biometric capture. Securlinx's approach centralizes the collection and continuous person matching functions no matter whether a fingerprint, finger/palm vein, facial image or iris scan is used separately, in combination or together with non-biometric data.

Securlinx's powerful solutions open the way for your organization to drive critical identity verification functions across all your operations and processes from a single platform that Integrates your systems, devices and workflow. That translates into a simpler, faster, more reliable way to validate and communicate identity data with confidence while reducing risk, complexity and cost.

The Securlinx biometric analytic components are designed with a narrow focus on biometric identity management and authentication. This enables the security and confidence of biometric validation to be added to a wide variety of applications while maintaining the simplicity of its value-add biometric identity management mission.



IdentiTrac data flow

Securlinx - IdentiTrac identity management consists of:

Biometric Edge Module Tasks

Enrollment: The gathering of biometric samples such as fingerprint, iris, face, finger-vein, etc., and pairing those samples with a unique identifier.

Authentication: The gathering of biometric samples to perform verifications and searches against the enrollment gallery while providing local recognition event notifications.

SecurLinx Cloud Service Tasks

Service Delivery: The upscaling of systems to meet surge and size demands as well as provisioning and availability management.

Central Matching: The creation, use, and secure storage of biometric templates and their paired identifiers especially across large populations.

Information Management: The clerical information housekeeping tasks related to maintaining the integrity of the data store and the continual improvement of enrollments.

Analysis Support: Features that assist the host system in anti-fraud efforts via de-duplication and information quality assurance via records linking. Custom flags and triggers in response to key recognition events are available.

Biometric Modalities and Future Proofing

Biometric modality is the phrase used to describe the type of biometric in use such as the two modalities of fingerprint and facial recognition. The term is useful because different biometric modalities have different characteristics of use. As a modality for example reliable, low-cost fingerprint recognition requires physical contact with a fingerprint reader but yields a very high confidence level while on the other hand the modality of facial recognition is an identity-at-a-distance technology whose quality of result is highly dependent upon the imaging environment.

Future proofing is the term that describes one of the benefits of using the SecurLinx model of a loosely coupled biometric identification management service. This allows the same Host Records Management System to participate in both fingerprint and facial recognition modalities, as well as iris, finger/palm vein, and others not yet invented, without detracting from its core mission of records management.

BioToken Design Benefit Analysis

The SecurLinx BioToken strategy is designed to:

- Decouple biometric modality and brand choices from the host record management system; Manage the enrollment and re-enrollment of BioTokens should changes be required.
- Increase the security of the identification data layer; Only encrypted BioTokens are exposed to the network.
- Reinforce work process flow; Can be used to implement role-based access and actions and provides firm audit trails.
- Investment protection; Allows plug-and-play connectivity for any biometric modality and brand for future flexibility.