tascent™

Tascent Enterprise Suite
Multimodal Biometric Identity Platform

Tascent Enterprise Suite
Multimodal Biometric Identity System
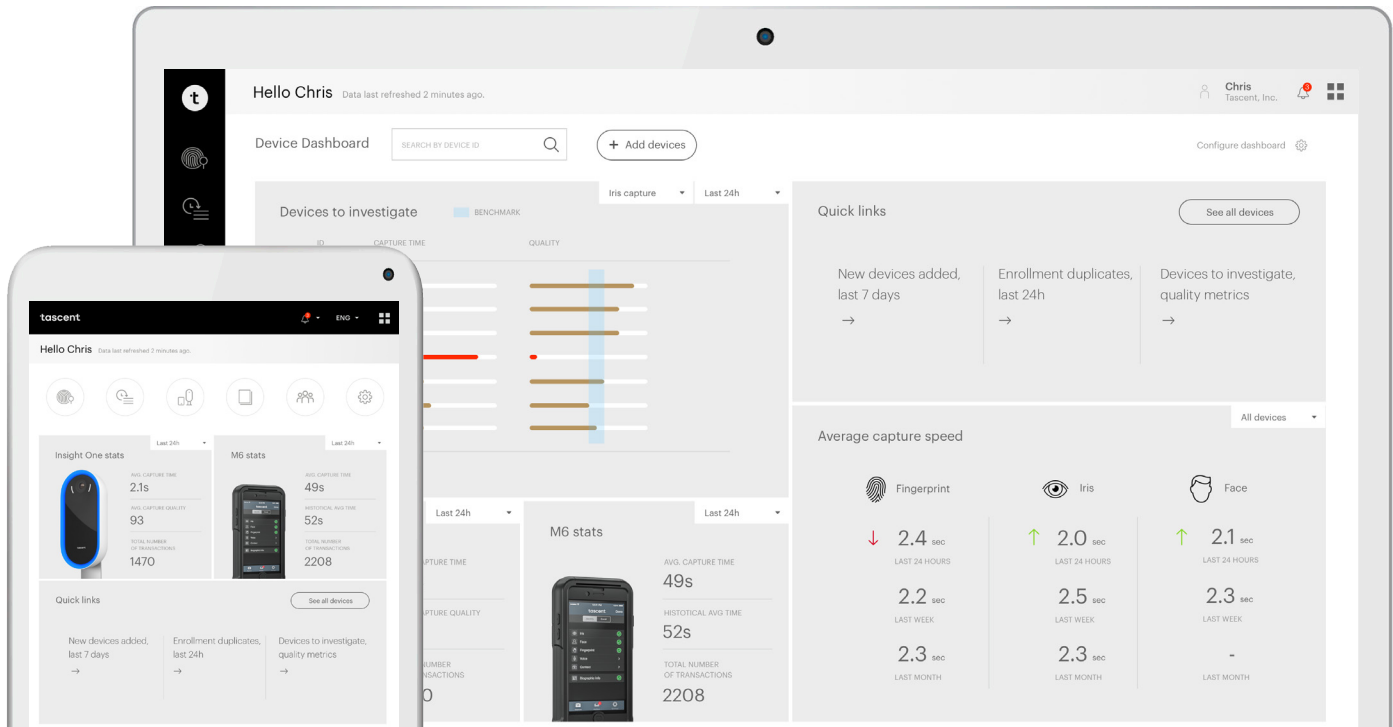
Secure, scalable, and easy-to-use, the Tascent Enterprise Suite represents a thoroughly modern approach to biometric identity systems. Delivering comprehensive identity capabilities in a way that's simple and intuitive, the Tascent Enterprise Suite makes it easy to deploy and manage an end-to-end biometric identity system. Out of the box, it provides a set of common identity services, including matching and data storage, immediately enabling seamless solutions using the Tascent ecosystem of devices and software services.

Thanks to a modular and open-architecture approach, the Tascent Enterprise Suite offers software components that can be easily integrated into existing identity systems as well as with third-party biometric devices. And leveraging standards-compliant image and data formats, it supports interoperability, future-proofing, and comprehensive access to identity records.

Versatile Biometric Identity System

• Deployable on premises or on cloud

• Provides enrollment and biometric identity data storage and management

• Open architecture and modular; integrates with external systems to transact identity data

• Integrates powerful analytics to drive actionable intelligence

Tascent Enterprise Suite
Solon Overview

●

Whether on-premises or in the cloud, the Tascent Enterprise Suite delivers powerful end-to-end biometric identity capabilities, enabling organizations to deploy, manage, and scale a complete identity solution with ease and simplicity.

Deploy a secure, scalable biometric identity system with ease:

▶ **Match with confidence**
Reliably match against iris, face, and fingerprint using advanced, scalable algorithms

▶ **Optimize enrollment**
Identity data management can be performed on desktop and mobile devices via user-friendly interfaces

▶ **Manage secure transactions**
Identities are securely translated, converted and routed through each step using industry-standard encryption

▶ **Drive actionable intelligence**
Intuitive tools provide robust data and analytics from identity and transactional data

▶ **Streamline device administration**
Easily configure and manage devices, apps, and edge data deployed across the enterprise
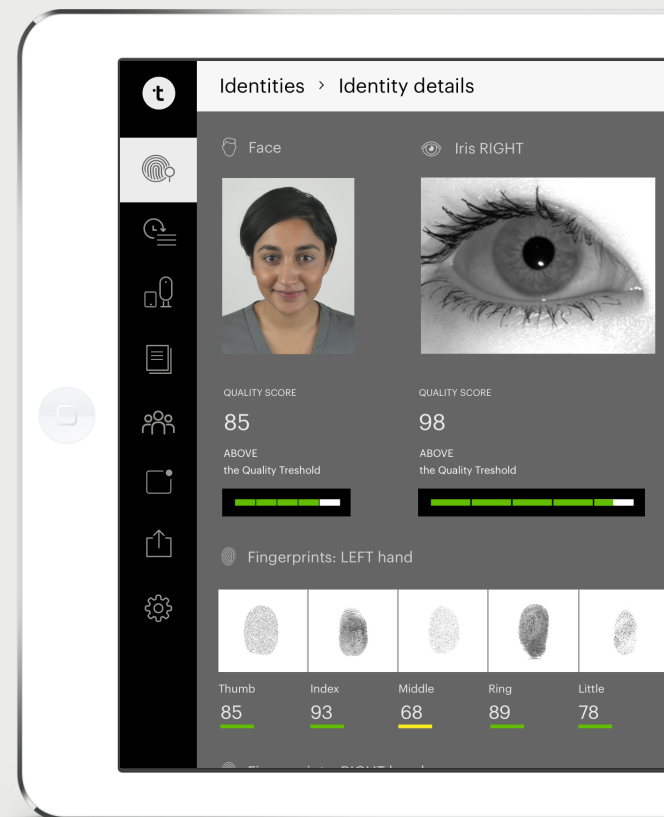
Tascent Enterprise Suite
Technical Overview

●

Tascent's modular and open-architecture approach enables organizations to deploy the complete Tascent Enterprise Suite out of the box, or easily integrate identity capabilities into their existing identity system. The following components power the Tascent Enterprise Suite.

Key Components:

Identity App Suite
Readily-customizable, user-friendly identity applications, optimized for both mobile and desktop scenarios

Frameworks
Clean, modular separation of key software and device components

Identity Engine
Multimodal biometric matching and storage

Transaction Manager
Translation, conversion, and routing of identity messages

Device Manager
Configuration & management of devices, apps, and edge data, deployed across the enterprise
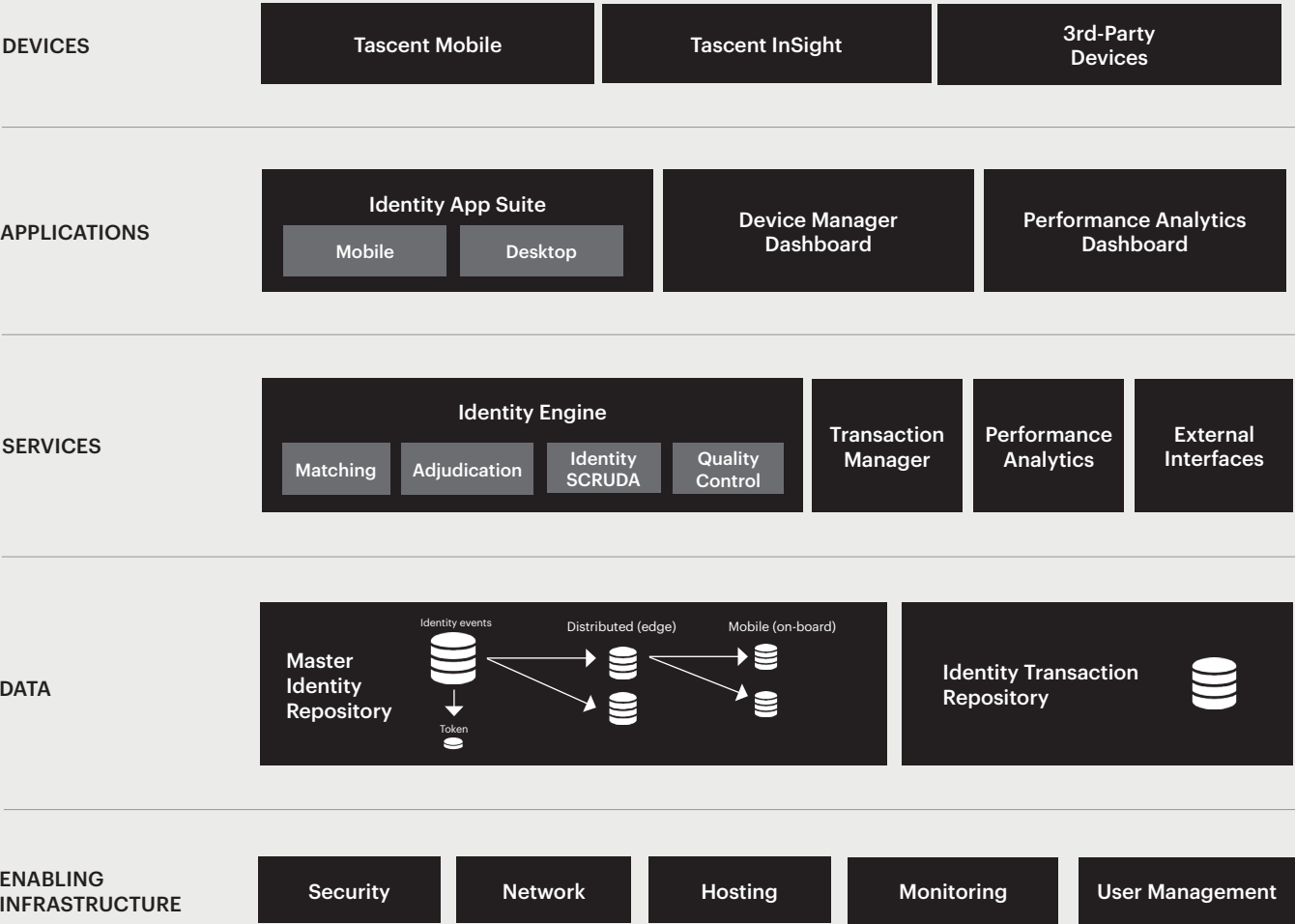
Performance Analytics
Actionable intelligence from identity and transactional data

Tascent Enterprise Suite
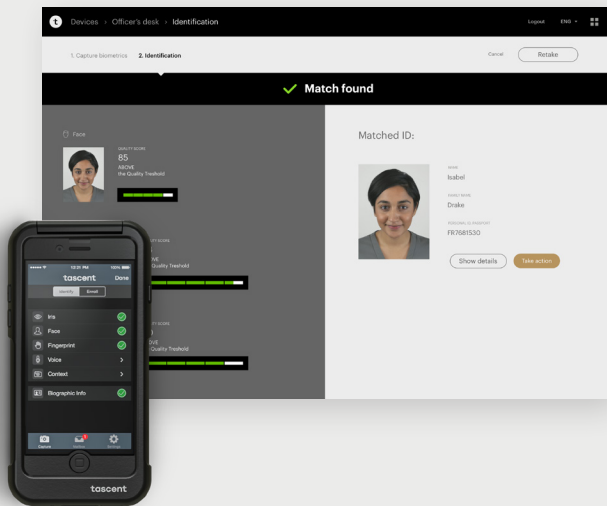## High-Level Architecture

The Tascent Enterprise Suite encompasses the full solution stack required to deploy a robust, scalable, and integrated biometric identity system. From enabling infrastructure to device endpoints, the Tascent Enterprise Suite considers complete system requirements while also integrating cleanly with existing capabilities.

Tascent Enterprise Suite High-Level Architecture:

DEVICES	Tascent Mobile	Tascent InSight	3rd-Party Devices

APPLICATIONS

Identity App Suite		Device Manager Dashboard	Performance Analytics Dashboard
Mobile	Desktop		

SERVICES

Identity Engine				Transaction Manager	Performance Analytics	External Interfaces
Matching	Adjudication	Identity SCRUDA	Quality Control			

DATA

Master Identity Repository — Identity events — Distributed (edge) — Mobile (on-board) — Token

Identity Transaction Repository

ENABLING INFRASTRUCTURE

Security	Network	Hosting	Monitoring	User Management

## Identity App Suite

User-friendly identity applications, optimized for both mobile and desktop scenarios, and readily customized to accommodate specific user requirements:

- Enrollment of iris, fingerprint, and face biometrics to the relevant ISO standards
- Mobile document capture and automated MRZ parsing from machine-readable travel documents (MRTDs)
- 1:N, 1:small-n, and / or 1:1 multimodal authentication
- On-board mobile identification against administrator-defined gallery subsets of up to 100k identities
- Assisted biometric adjudication of edge cases, with feedback enabling effective tuning of matching parameters
- Simplified Identity Management, including search, update, delete/archive, and import / export of identities, individually or in bulk
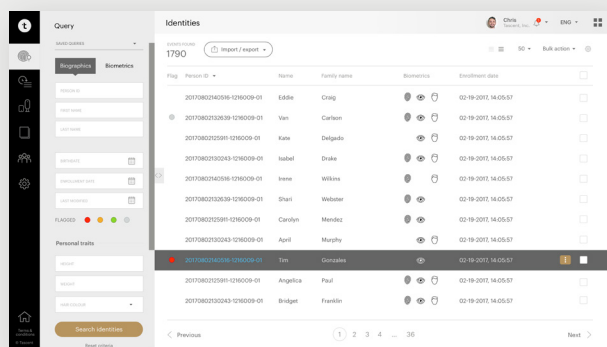
Identity Engine

Server-based multimodal biometric matching and storage

- Accurate, scalable matching and fusion of iris, fingerprint, and face biometrics, using interchangeable third-party algorithms
- Storage and signing of original identity enrollment records to assure future-proofing
- Synchronization of configurable subsets of identity data to edge devices according to defined schedule and device availability
- Biometric quality checking of iris, fingerprint, and face using multiple granular parameters (ISO / ICAO compliance enforced)
- Retention of identity event history, and ability to roll-back changes

Performance Analytics

Intuitive tools and powerful visualizations to drive actionable intelligence from identity and transactional data

- Static, predefined reports for common tasks; readily-customizable ad-hoc reporting according to user requirements
- Real-time monitoring of system biometric matching activity and performance
- Geographic visualization of identity events, overlaid with multiple layers of transaction data
- Predictive maintenance of biometric devices according to key performance criteria
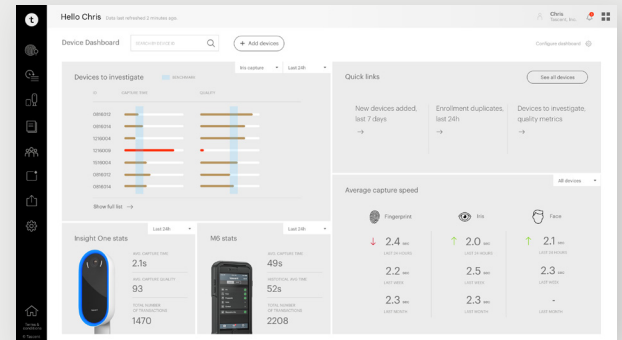
Transaction Manager

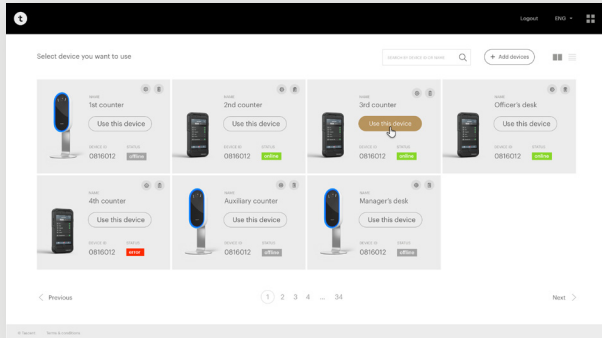Translation, conversion, and routing of identity messages

- Rules-based transaction management, enabling ready addition, removal, and editing of major identity workflows via GUI
- Identity record conversion between native and standardized formats (including ANSI-NIST ITL-1 XML and FBI-CJIS / DoD EBTS)
- Option to store and retrieve all source and translated messages (including raw images) in their original form
- Web services-based interfacing with existing AFIS / ABIS systems

Device Manager

Streamlined configuration & management of devices, apps and edge data, deployed across the enterprise

- Centralized monitoring of device location, health, and usage
- App configurations pushed out and locked-down according to user profiles
- Consolidated central logging of device transactional and performance data, uploaded according to admin-defined rules
- Complements leading third-party MDM/MAM products for security and convenience - app updates pushed out according to user profiles, device availability, and central scheduling
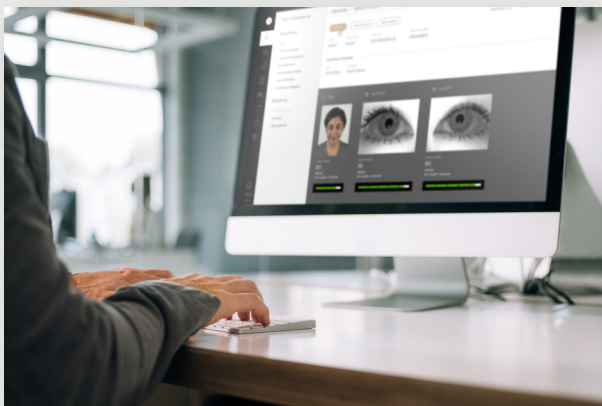
Frameworks

Clean, modular separation of key components simplifies maintenance and expansion

- **Devices:** Standards-based web services and a cross-platform developer SDK provides future-proofing and vendor-independence; hardware decisions are insulated by Tascent's abstraction frameworks
- **Algorithms and Matchers:** Snap-in / snap-out of matching and other biometric functionality between vendors and versions
- **Operations:** Standardized SNMPv3-based monitoring for easy integration into existing operational tools

Tascent Enterprise Suite

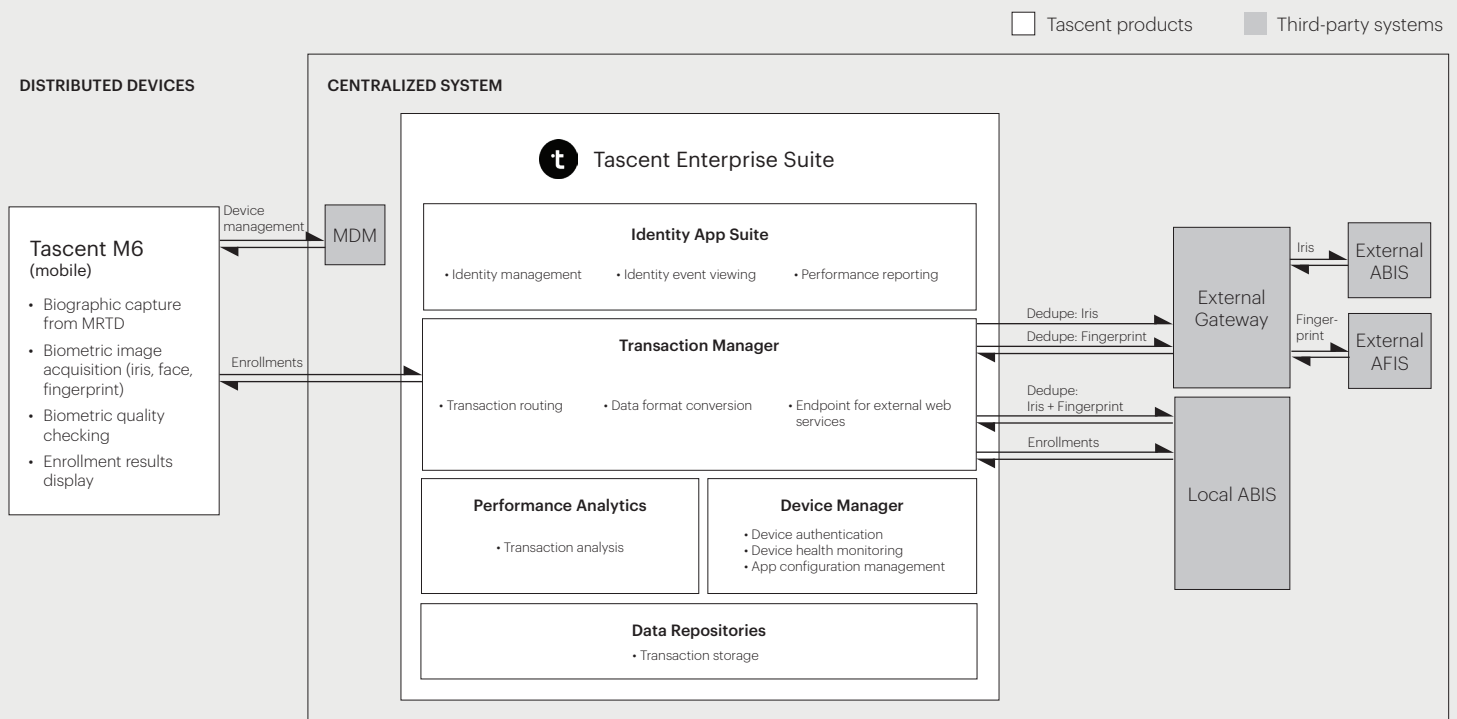Deployment Example: Mobile Enrollment with Existing Identity System

The Tascent Enterprise Suite's modular, open architecture approach allows it to seamlessly integrate into environments with existing identity capabilities and enabling infrastructure.

In this deployment scenario, the Tascent M6 mobile device and the Tascent Enterprise Suite is integrated into the Client's current identity system to deliver fast, accurate Mobile Enrollment capabilities.

Concept of Operations

1. Biometric and biographic data is captured on M6, and validated / quality-checked.

2. Enrollment requests are created, stored locally, and sent to the server using 4G / LTE / WiFi as connectivity is available.

3. The Transaction Manager stores the transaction, converts it into multiple separate identification requests, and sends them to the Client's existing backend AFIS/ABIS systems.

4. The Client's AFIS/ABIS systems perform identity deduplication, and return responses to the Transaction Manager.

5. Once deduplication responses are returned, the Transaction Manager correlates the results. If no duplicate identity is found, the Transaction Manager triggers an Enrollment request to the Client's local ABIS.

6. Enrollment results are returned to the Mobile App and displayed to the operator. Watchlists are prioritized.

7. Fundamental performance analytics enable identity transaction reporting based on activity type, time, location, user, etc..

Functional Overview Diagram

□ Tascent products   ▦ Third-party systems

DISTRIBUTED DEVICES

CENTRALIZED SYSTEM

Tascent Enterprise Suite

Identity App Suite
- Identity management
- Identity event viewing
- Performance reporting

Transaction Manager
- Transaction routing
- Data format conversion
- Endpoint for external web services

Performance Analytics
- Transaction analysis

Device Manager
- Device authentication
- Device health monitoring
- App configuration management

Data Repositories
- Transaction storage

Tascent M6 (mobile)
- Biographic capture from MRTD
- Biometric image acquisition (iris, face, fingerprint)
- Biometric quality checking
- Enrollment results display

Device management → MDM

Enrollments

Dedupe: Iris
Dedupe: Fingerprint

External Gateway

Iris → External ABIS
Fingerprint → External AFIS

Dedupe: Iris + Fingerprint
Enrollments

Local ABIS

Tascent Enterprise Suite
Deployment Example: End-to-End Biometric Identity System

In this deployment scenario, the Tascent Enterprise Suite functions as the end-to-end biometric identity system, providing mobile enrollment with on-board identification capabilities, high throughput identification, and central biometric matching and identity management.

Concept of Operations

Mobile Enrollment

1. A minimum set of biometric and biographic data is captured on M6, and validated / quality-checked.
2. Enrollment requests are created and stored locally, if working offline.
3. When M6 comes online, enrollments are forwarded to the server for deduplication.
4. Transaction Manager routes requests to Identity Engine and stores transaction.
5. The Identity Engine performs multimodal 1:N deduplication and returns the results.
6. Transaction Manager updates transaction and returns results to M6. If no duplicate is identified, it triggers creation of a new identity in Master Identity Repository.
7. Enrollment results are available on the M6 for operator review.

Mobile Identification

1. A minimum set of biometrics are captured on M6 and quality-checked.
2. Identification requests are created, and irises and/or fingerprints are matched against the on-board database, working offline.
3. Top-n candidate lists are available for operator review; any watchlist hits raise alerts for immediate operator attention.
4. When M6 comes online, on board identity database is auto-updated.

High-Throughput Identification

1. InSight One device captures high-quality iris and face biometric images.
2. Identification requests are sent to centralized system.
3. Transaction Manager routes requests to the Identity Engine, and stores transaction.
4. Identity Engine performs rapid 1:N identification and returns results.
5. Transaction Manager updates transaction and returns results to InSight One.
6. InSight One displays the outcome to the user via its LCD / LED user interface.

Functional Overview Diagram
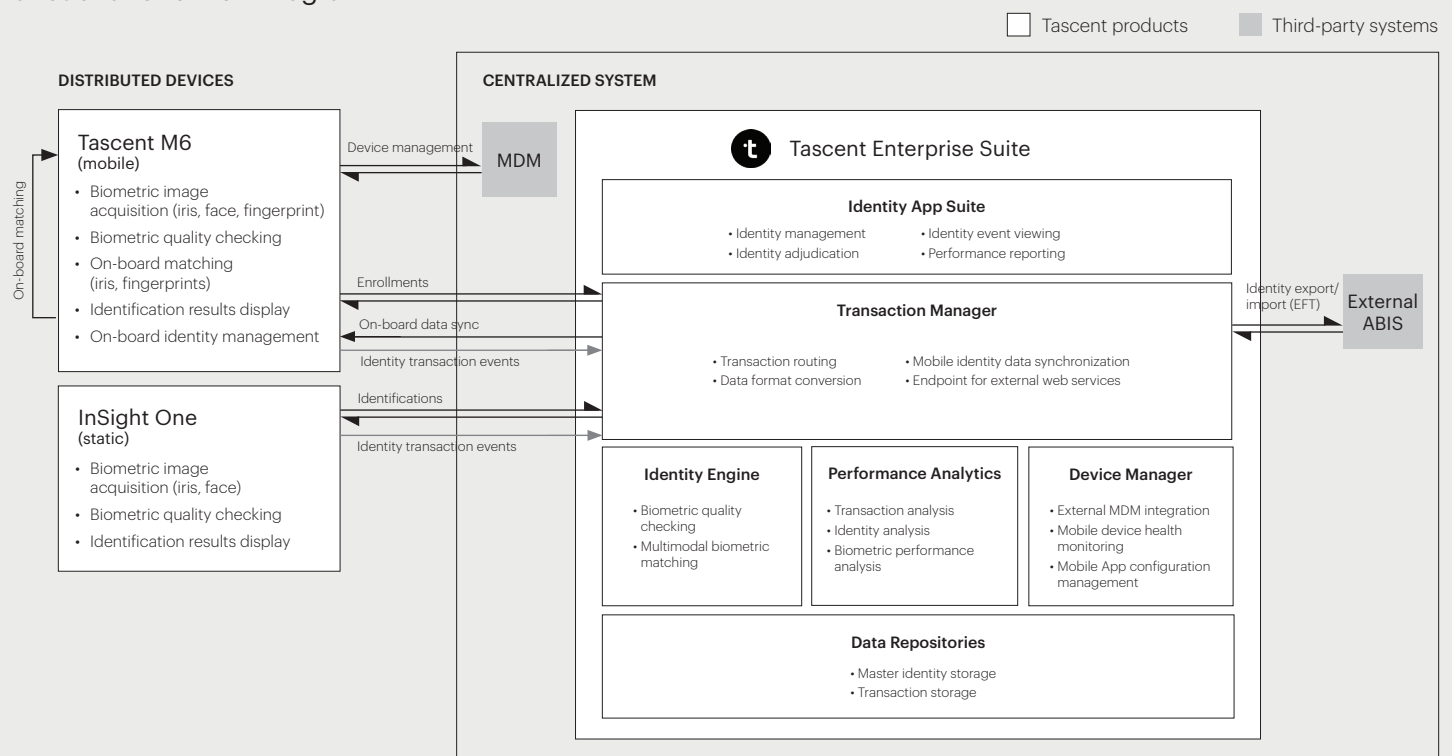
BIOMETRIC SPECIFICATIONS

Parameter	Value / Functionality
Modalities	Fingerprint, face, iris enabled as standard Additional modalities supported by request
Identity Database Size	System deployable in steps of 1M / 10M / 100M unique identities Pilot system sizing of up to 100k identities is also available
Biometric Standards Support	Deployable in compliance with: • ANSI/NIST-ITL-1 • FBI/CJIS EBTS 10.0 • ISO/IEC 19794

SYSTEM SPECIFICATIONS

Parameter	Value / Functionality
Deployment Options	Deployable onto a range of infrastructures: • Physical hardware (on-premises) • Private virtualized • Public cloud (AWS or equivalent) Horizontally scalable to meet specific transaction throughput requirements.
Data Synchronization	Synchronize key identity data with up to 50 mobile or edge devices in parallel. Data sync rate in excess of 20 identities/s (72k identities/hour).
Interfaces	Web services for biometric Matching and identity management derived from OASIS-BIAS standard. Lightweight JSON interface optimized for high-speed Data Sync.

SECURITY AND PRIVACY

Parameter	Value / Functionality
Security	Deployable in compliance with: • FIPS 140-2 • Criminal Justice Information Services (CJIS) Security Policy v5.5 PKI-based mutual authentication of servers and endpoints Data-in-transit: AES-256 CBC symmetric cryptography; transport layer is further secured using HTTPS (TLS 1.2) Data-at-rest: AES-256-based whole-disk encryption Mobile devices secured by industry-leading MDM capabilities
Privacy	Deployable in compliance with: • ISO/IEC 24745:2011, Information technology – Security techniques – Biometric information protection • British Standards Institution PAS92:2011 – Code of Practice for the Implementation of a Biometric System • Biometrics Institute Biometrics Privacy Guidelines (2015) A sample Privacy Impact Assessment of an illustrative deployment is available upon request

·tascent·

Tascent, Inc.

475 Alberto Way

Los Gatos, CA 95032

T 408 335 4700

-

www.tascent.com

·tascent·