Contact, Non-Contact, and Passive Resolution Modes for Biological Identity

by Nick Clark | Published March 27, 2026 | PDF

Biological identity verification does not require a single interaction modality. The architecture defines three distinct resolution modes, each with different signal quality characteristics, consent requirements, and operational profiles. Contact, non-contact, and passive modes operate under a unified governance framework with explicit escalation protocols between them.

What It Is

Three resolution modes define how biological signals are acquired. Contact mode requires physical interaction between the subject and a sensor, such as fingerprint or palm vein scanning. Non-contact mode uses sensors that operate at a distance, such as facial geometry or iris recognition. Passive mode observes behavioral patterns without any deliberate interaction, such as gait analysis or typing dynamics.

Each mode produces signals with distinct quality characteristics. Contact signals are highest fidelity but most intrusive. Passive signals are least intrusive but noisiest. The architecture treats these as complementary rather than competing approaches.

Why It Matters

Most biometric systems commit to a single modality at design time. A fingerprint reader cannot fall back to voice recognition. An iris scanner cannot gracefully degrade to gait analysis. This rigidity creates failure modes where the system either works perfectly or fails completely.

Multi-modal resolution with governed escalation means the system can begin with the least intrusive mode and escalate only when additional confidence is needed. Consent gates at each transition ensure the subject retains control over which biological signals are observed.

How It Works Structurally

The system evaluates the current trust slope against the authorization threshold for the requested operation. If passive observation provides sufficient confidence, no escalation occurs. If confidence is insufficient, the system requests escalation to non-contact mode with explicit consent. Further escalation to contact mode follows the same pattern.

Each mode contributes to the same underlying trust slope. Observations from different modes are fused through cross-modal integration while maintaining mode-specific quality metadata. The escalation protocol records each transition in the identity lineage.

What It Enables

Consent-gated multi-modal resolution enables identity systems that adapt to context. A low-security area may operate entirely in passive mode. A high-security zone may require contact verification but only when the passive slope is insufficient. The subject always knows which modes are active and retains the ability to refuse escalation, accepting the corresponding access limitation.

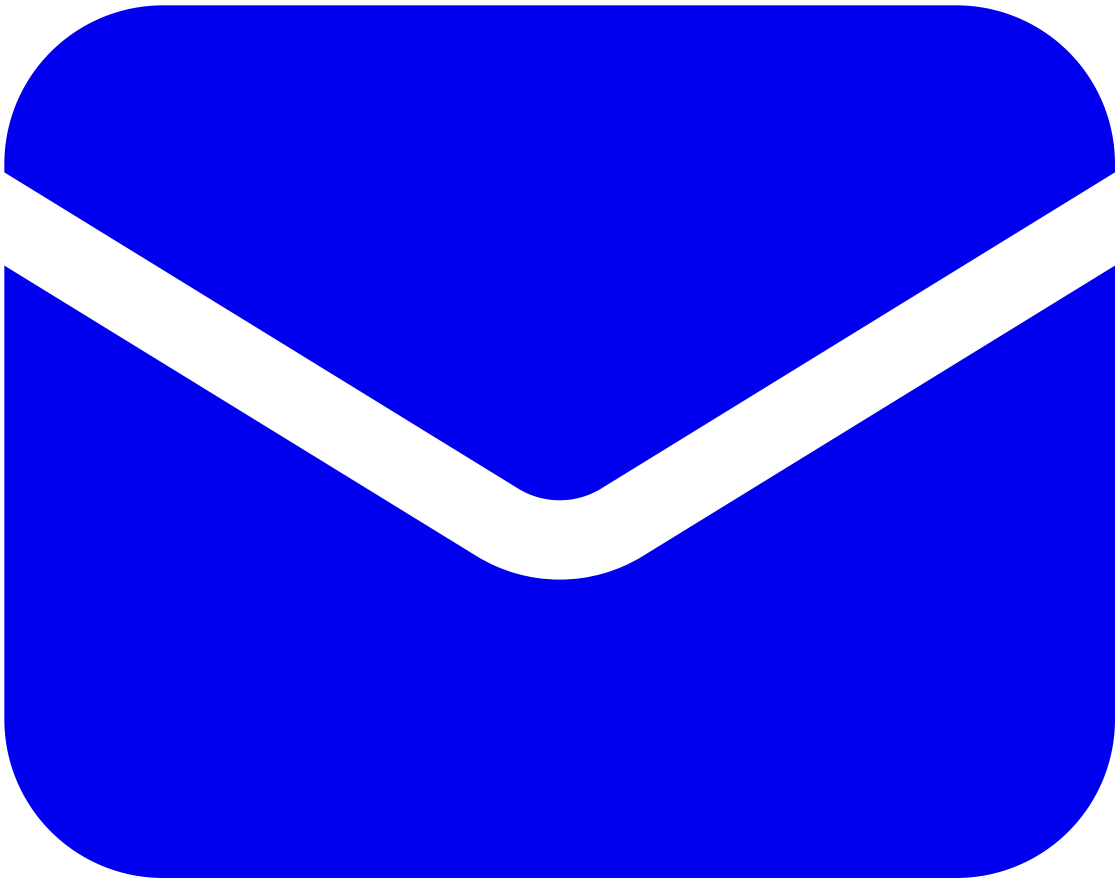
Biological Identity All 21 steps →

Identity from behavioral continuity. No stored templates. No keys.

Primary Technical Disclosure
○ Continuity-Based Biological Identity Using Trust-Slope Validation
Secondary Technical
○ Biological Trust Slope Construction: Identity Through Behavioral Continuity● Contact, Non-Contact, and Passive Resolution Modes for Biological Identity○ Biological Hash Generation With Domain Separation○ Biological State Inference From Continuity Baseline○ Cross-Modal Biological Hash Fusion○ Biological Continuity as Handoff Verification○ Relational Trust Trajectories: Trust as Temporal Relationship○ Identity as Behavioral Continuity: Beyond Single-Point Capture○ Biological-Device-Agent Identity Layering○ Biological Signal Acquisition Tiers○ Noise-Tolerant Feature Normalization for Biological Signals○ Stable Sketching and Helper Data for Biological Features○ Predictive Identity Trajectory: Forecasting Biological Identity Evolution○ Population-Scale Collision Resistance for Biological Hashes○ Adaptive Indexing of Biological Trust Slopes○ Delayed and Sparse Validation for Disconnected Environments○ Policy-Governed Capability Binding for Biological Identity○ Multi-Identity Delegation Without Biological Data Disclosure○ External Credential Integration With Trust-Slope Integrity○ Anti-Spoofing Through Continuity Validation○ Identity Lifecycle Management and Phase-Based Reseeding○ Quorum-Based Biological Identity Recovery○ Privacy Governance and Revocation for Biological Identity○ Human-Agent Primitive Integration for Biological Identity
Applications (General)
○ Airport Security Without Biometric Databases○ Estate Verification Through Behavioral Continuity○ Biological Identity for Elder Care Continuity○ Biological Identity for Child Development Tracking○ Biological Identity for Addiction Recovery Monitoring○ Biological Identity for Workplace Safety Monitoring○ Biological Identity for Athletic Performance○ Biological Identity for Immigration Processing
Applications (Specific)
○ TSA PreCheck Matches Templates, Not Continuity○ Global Entry Verifies Documents, Not Biological Continuity○ Face ID Matches a Stored Model, Not a Living Trajectory○ Samsung Knox Guards the Container, Not the Identity○ ID.me Verifies Documents, Not Biological Continuity○ Socure Scores Risk at a Single Point in Time○ Plaid Identity Verifies Financial Accounts, Not Biological Persons○ Onfido Detects Document Fraud, Not Identity Drift○ Veriff Captures Sessions, Not Trajectories○ Trulioo Queries Databases, Not Biological Trajectories
Biological Identity overview →
AQ
deterministic
autonomy

Legal

Last updated: 2026-03-03



-
- nick@qu3ry.net
- 72 28 14 36 01

Invented by Nick Clark | Founding Investors: Devin Wilkie