Biological Signal Acquisition Tiers

by Nick Clark | Published March 27, 2026 | PDF

Biological signals vary enormously in quality depending on how they are acquired. The architecture defines three acquisition tiers, contact, semi-contact, and non-contact, each producing signals with characteristic fidelity, noise profiles, and operational constraints. Understanding these tiers as a structured hierarchy rather than competing alternatives enables identity systems that adapt their acquisition strategy to operational requirements.

What It Is

The three acquisition tiers define a structured hierarchy of biological signal quality. Contact tier involves direct physical interaction between the subject and a sensor, producing the highest-fidelity signals. Semi-contact tier involves proximity-based sensing without direct touch. Non-contact tier involves observation at a distance or through passive behavioral monitoring.

Each tier has characteristic signal-to-noise ratios, environmental sensitivity, and throughput limitations. These characteristics are not limitations to overcome but parameters to govern. The architecture treats signal quality as a first-class input to identity confidence computation.

Why It Matters

Most biometric systems are designed around a single acquisition tier. A fingerprint reader is a contact system. A facial recognition camera is a non-contact system. When the system's tier is inappropriate for the environment, the system fails. A fingerprint reader fails outdoors in rain. A facial camera fails in darkness.

Tier-aware acquisition enables the system to select the most appropriate modality for current conditions and to explicitly account for signal quality when computing identity confidence. A low-quality non-contact observation contributes less to the trust slope than a high-quality contact observation, and the system knows this quantitatively.

How It Works

Each acquisition event is tagged with its tier and a quality metric reflecting signal fidelity. The feature extraction pipeline applies tier-specific normalization to account for the characteristic noise profile of each tier. The trust slope accumulation function weights observations by their quality-adjusted contribution.

Tier transitions are governed by policy. Escalation from non-contact to contact requires consent. De-escalation from contact to non-contact occurs naturally when contact sensors are unavailable. The system maintains identity continuity across tier transitions by ensuring the underlying trust slope is tier-agnostic even though individual observations are tier-specific.

What It Enables

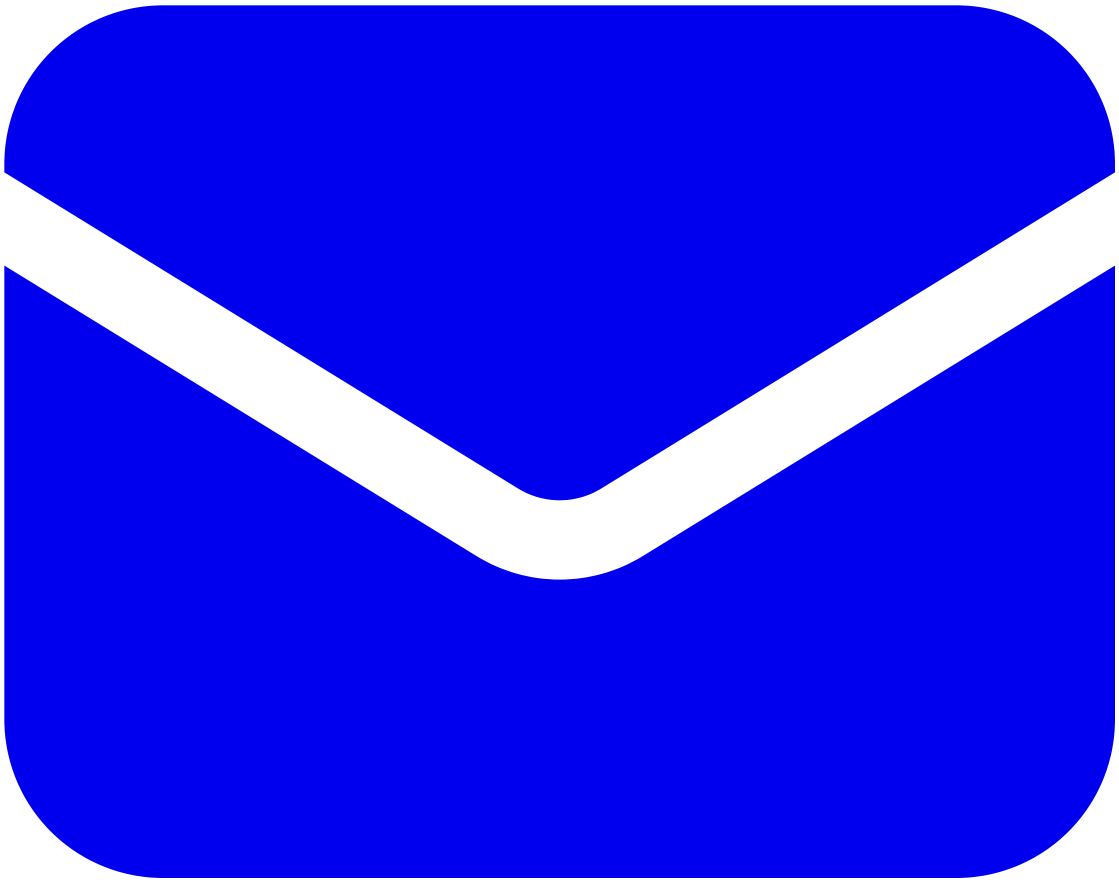
Tier-aware acquisition enables identity systems that operate across diverse environments with explicit quality accounting. A single identity framework can govern entry to a building using contactless observation at the door, contact verification at a security checkpoint, and passive behavioral monitoring throughout the facility, all contributing to the same trust slope with appropriate quality weighting.

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

Last updated: 2026-03-03



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

Invented by Nick Clark | Founding Investors: Devin Wilkie