Face ID Matches a Stored Model, Not a Living Trajectory

by Nick Clark | Published March 27, 2026 | PDF

Apple's Face ID represents the most widely deployed facial authentication system. The TrueDepth camera projects thousands of infrared dots to create a mathematical model of the user's face, and authentication compares the current face against this model. The engineering is exceptional: fast, reliable, and resistant to common spoofing attacks. But Face ID verifies that the current face matches a stored mathematical model. It does not validate that the user's biological identity trajectory is consistent with the legitimate device owner over time. The distinction matters for the authentication challenges that lie ahead.

What Apple built

Face ID combines structured-light depth mapping with neural network processing in the Secure Enclave to achieve facial authentication with a one-in-a-million false acceptance rate. The system adapts its stored model incrementally to account for changes in appearance: haircuts, glasses, aging. The mathematical model never leaves the device. The security architecture ensures that the biometric data is isolated from the application processor and from Apple's servers.

Authentication is a comparison: does the current face, as measured by the TrueDepth camera, match the stored mathematical model within acceptable tolerances? Successful matches are recorded but not analyzed for trajectory consistency. Each authentication is independent of the previous one.

The gap between matching and trajectory validation

Face ID's adaptation mechanism updates the stored model to track gradual appearance changes. This is a valuable capability that prevents false rejections as the user's face naturally evolves. But the adaptation is local: each successful match slightly adjusts the model. It does not maintain a trajectory of biological identity that can detect anomalous patterns across authentication events.

The distinction matters as spoofing techniques advance. Current Face ID is resistant to photos, masks, and basic 3D printed faces. But the arms race between authentication and spoofing is ongoing. A sophisticated spoof that defeats a single authentication event may not defeat trajectory analysis because the spoof cannot reproduce the authentic user's biological evolution pattern. The real user's face changes in predictable ways informed by their biology. A spoof, even a good one, follows a different trajectory or no trajectory at all.

The stored model also represents a single point of vulnerability. If the Secure Enclave is compromised, the mathematical model is exposed. Trajectory-based identity does not depend on a stored model that can be extracted. Identity is the trajectory itself, accumulated through genuine interactions.

What biological identity enables for device authentication

With trust-slope trajectory validation, each Face ID authentication contributes to a biological identity trajectory. The system validates not just geometric similarity but trajectory consistency: is the biological evolution pattern consistent with the same individual over time? The trajectory incorporates subtle signals beyond facial geometry: micro-expression patterns, physiological indicators detectable through existing sensors, and behavioral patterns during the authentication gesture.

State inference from the trajectory enables contextual authentication. The system can detect not just who is authenticating but their current physiological state. Authentication under duress may exhibit biological patterns inconsistent with the user's normal trajectory, triggering additional security measures without requiring the user to take explicit action.

The structural requirement

Face ID's authentication security is industry-leading for template-based biometrics. The structural gap is between matching and trajectory. Biological identity provides continuity-based validation that accumulates security over time, detects sophisticated spoofs through trajectory analysis, and eliminates dependence on stored templates. The device authentication system that validates biological trajectory is structurally more resilient than one that matches against a stored model, regardless of how well-protected that model is.

Biological Identity All 21 steps →

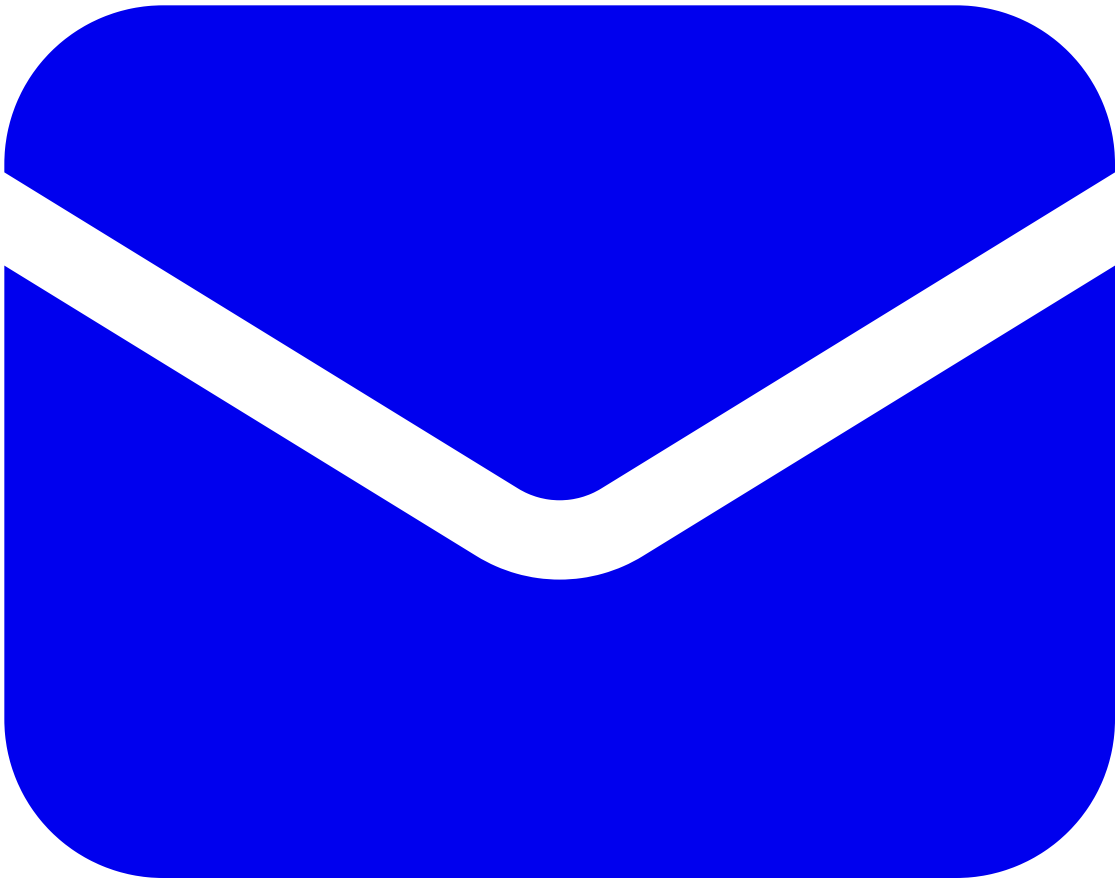
Identity from behavioral continuity. No stored templates. No keys.

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

Subject to one or more pending U.S. and international patent applications, see Patents for the current list and status. No license, express or implied, is granted. Any use requires a separate written agreement—see Licensing. Patent applications referenced on this site are pending. Claim scope, if any, is subject to examination and may issue in altered form or not at all. See Legal for terms and conditions.

Last updated: 2026-03-03



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

Invented by Nick Clark | Founding Investors: Devin Wilkie