ID.me Verifies Documents, Not Biological Continuity

by Nick Clark | Published March 28, 2026 | PDF

ID.me built a federated identity verification network that serves government agencies, healthcare systems, and enterprises. The platform authenticates documents and matches selfies against government-issued photo IDs. The verification works for its intended purpose: confirming that a person holds valid credentials at a single moment. But it validates credential possession, not biological continuity. The structural gap is between proving you hold the right document and proving you are the same person across time.

What ID.me built

ID.me provides identity proofing and group verification for access to government benefits, tax filing, healthcare portals, and commercial services. The platform's verification flow asks users to photograph a government-issued ID, take a selfie, and submit both for automated comparison. Machine learning

models compare facial geometry between the selfie and the document photograph. If the comparison exceeds a confidence threshold, identity is verified. If not, the user is routed to a video call with a human verifier.

The model is fundamentally document-centric. The ground truth is the government credential. The biometric comparison anchors the person to the credential at the moment of verification. Nothing in the system tracks whether the person's biological identity trajectory is consistent across multiple verification events over months or years. Each verification is an independent event that does not inform or validate subsequent verifications.

The gap between credential verification and biological continuity

Document-based verification answers one question: does this person hold a valid credential right now? Biological continuity answers a different question: is this person's trajectory of biological signals consistent with the individual they claim to be across an accumulated history of interactions?

The distinction has practical security consequences. A compromised document paired with a sufficiently similar face can defeat single-session verification. Synthetic media capable of generating plausible selfies creates an adversarial surface that grows more capable each year. The verification system's reliance on a single comparison point means it must win every encounter against improving attack surfaces.

Biological continuity shifts the security model. An attacker who defeats a single biometric comparison still cannot produce a trajectory of biological signals consistent with the legitimate individual's accumulated history. The trajectory includes behavioral patterns at verification, physiological consistency across sessions, and the natural evolution of biological signals over time. Spoofing a moment is categorically different from spoofing a trajectory.

What biological identity enables for civic verification

With trust-slope trajectory validation, each interaction with an identity verification system contributes to an accumulated biological trajectory. A person verifying identity for tax filing in January, healthcare access in March, and benefit renewal in August accumulates a trajectory that validates itself through consistency. The system does not compare against a stored template. It validates that the current interaction is consistent with the trajectory accumulated across all prior interactions.

Stable sketching means no biometric database is necessary. Biological signals are transformed into compact representations that support trajectory validation without enabling reconstruction of the original data. The privacy vulnerability inherent in centralized biometric databases is eliminated structurally rather than through access controls.

Post-quantum resilience follows from the architecture. Identity does not depend on cryptographic primitives that quantum computing could break. Continuity-based biological identity derives from accumulated behavioral and physiological trajectory, which is not a mathematical problem amenable to quantum attack.

The structural requirement

ID.me solved federated identity verification for document-centric workflows. The structural gap is between single-session credential validation and trajectory-based biological continuity. Biological identity provides verification that strengthens over time rather than resetting at each encounter, eliminates the need for stored biometric templates, and resists the synthetic media attack surface that document-matching systems must perpetually defend against. The identity system that validates trajectory is structurally more secure than one that matches selfies against credentials.

Biological Identity All 21 steps →

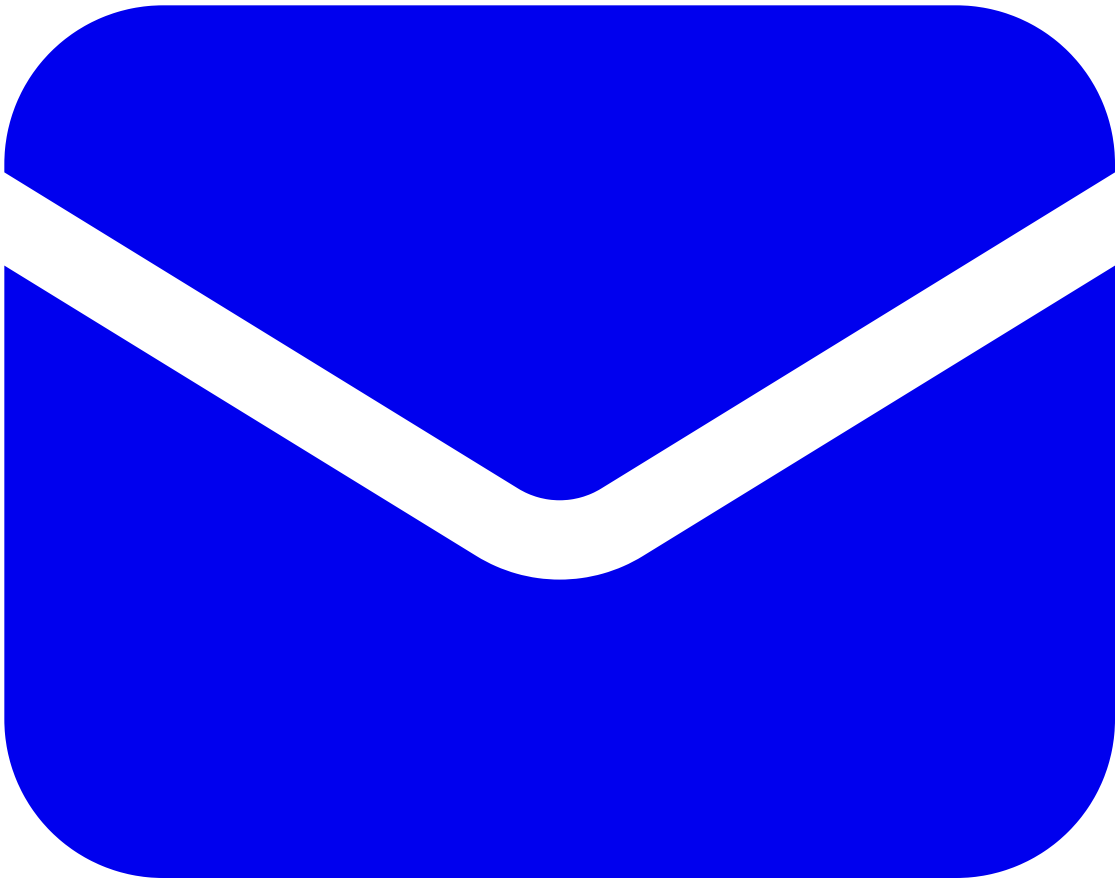
Identity from behavioral continuity. No stored templates. No keys.

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