Biological-Device-Agent Identity Layering

by Nick Clark | Published March 27, 2026 | PDF

Identity in the architecture operates at three distinct layers: biological (human), device (DDH), and agent (DAH). Each layer has independent trust slopes, independent governance, and independent lifecycle management. The interactions between layers are explicitly defined, preventing conflation of human identity with the devices they use or the agents that act on their behalf.

What It Is

The three-layer identity model separates biological identity (the human), device identity (the Dynamic Device Hash or DDH), and agent identity (the Dynamic Agent Hash or DAH) as independent but interacting identity substrates. Each layer maintains its own trust slope, its own continuity validation, and its own governance policies.

Biological identity represents the physical human through behavioral continuity. Device identity represents the computational substrate through hardware-derived entropy. Agent identity represents the software entity through its mutation history and memory state.

Why It Matters

Conflating identity layers creates fundamental security vulnerabilities. If device identity is treated as human identity, a stolen device becomes a stolen identity. If agent identity is treated as human identity, a compromised software agent can impersonate its operator. Separating the layers ensures that compromise of one layer does not automatically compromise the others.

The separation also enables independent lifecycle management. A human's biological identity persists across device changes. A device's identity persists across agent installations. An agent's identity persists across substrate migrations.

How It Works

Each layer produces its own identity hash through its own derivation pipeline. Cross-layer binding occurs through slope entanglement: the biological trust slope is bound to specific device trust slopes, and device trust slopes are bound to specific agent trust slopes. These bindings are verifiable but the bound slopes remain independently evaluable.

When a human operates a device running an agent, all three layers are active and their slopes are entangled. The system can verify that a specific human is operating a specific device running a specific agent without any single layer having access to the others' raw identity material.

What It Enables

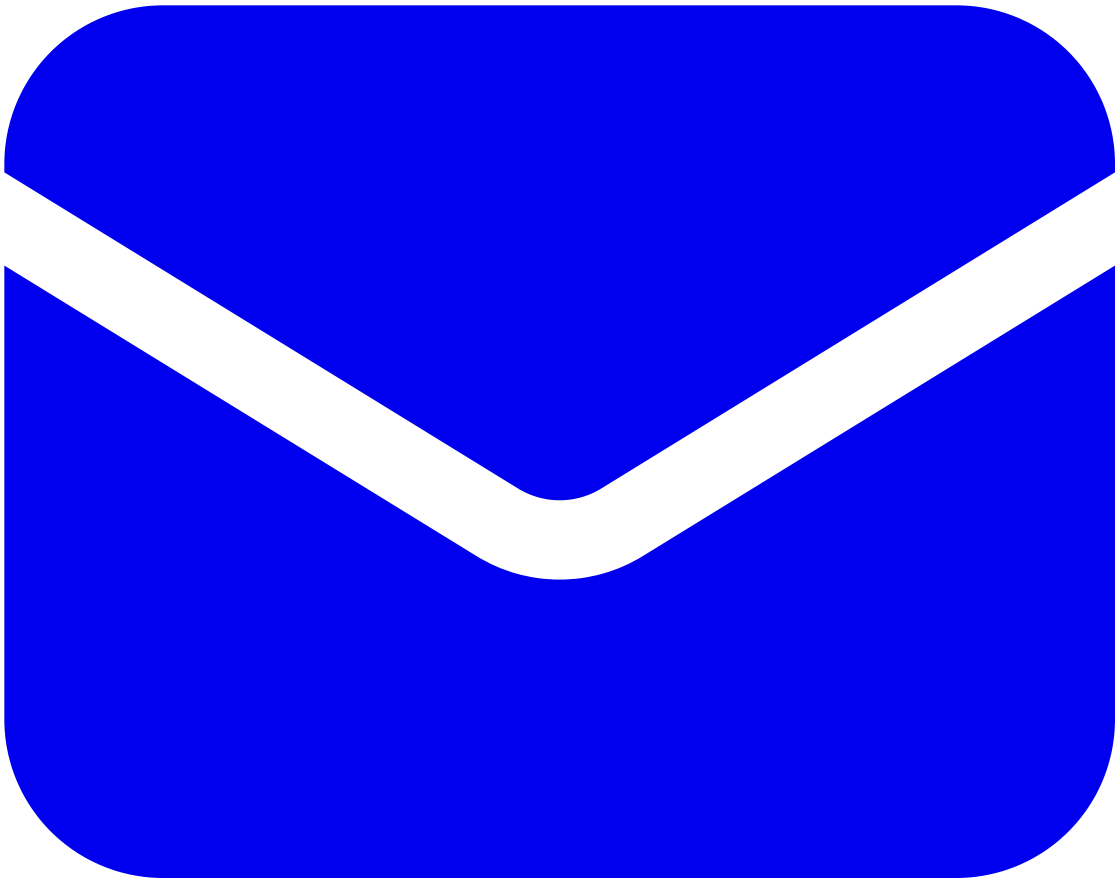
Three-layer identity enables precise authorization: you can authorize a specific human on any device, a specific device with any operator, or a specific agent regardless of where it runs. Cross-layer policies can require all three layers to align for high-security operations while allowing single-layer verification for low-security ones. The architecture naturally supports the full spectrum from anonymous device interaction to fully attributed human operation.

Biological Identity All 21 steps →

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

Legal

Last updated: 2026-03-03



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

Invented by Nick Clark | Founding Investors: Devin Wilkie