Continuity-Identity Processor IC: Silicon-Block Embodiment

by Nick Clark | Published April 25, 2026

What the IC Specifies

The continuity-identity processor IC integrates: a hash-chain accumulator that computes successor hashes from prior credentialed state, a trust-slope evaluator that weighs observed identity-relevant signals against the credentialed baseline, signature primitives for credential continuity verification, secure storage for the device's current identity state, and externally-observable telemetry for governance-credentialed monitoring.

The IC is silicon: a discrete chip or an IP block integrated into a larger SoC. It operates as the trust-evaluation primitive for the device that contains it, providing identity attestation as a hardware-grounded operation rather than a software-grounded one.

Why Silicon-Layer Embodiment Matters Architecturally

Continuity-based identity at the software layer is implementable but not unforgeable. A sophisticated attacker who compromises the device's software can produce arbitrary identity attestations regardless of the underlying continuity logic. The

protection is bounded by software-attack-surface security, which scales poorly across the device population.

Silicon-layer embodiment changes the attack surface. The continuity-identity logic operates in hardware, with its state and computation isolated from the software environment. Compromising the software does not compromise the identity attestation; the attacker must compromise the silicon, which is structurally harder.

How the IC Composes With Existing Secure Elements

The IC operates additively with existing secure-element architectures. Conventional secure elements (TPMs, secure enclaves, secure microcontrollers) provide cryptographic key storage and signing primitives. The continuity-identity IC consumes these primitives and adds the trust-slope evaluation, hash-chain accumulation, and credentialed-monitoring logic that continuity-based identity requires.

The integration is technology-neutral. The IC can operate with any underlying signing-primitive technology (ECDSA today, post-quantum tomorrow). Migrating between cryptographic schemes does not require re-architecting the IC's continuity logic; only the underlying primitives change.

What This Enables for Hardware Identity Across Domains

Automotive electronics gain continuity-based identity that operates across vehicle ECUs without requiring per-ECU software-level trust reconstruction. Defense electronics gain hardware-grounded identity that survives software-level compromise. Medical devices gain continuity-based device identity that supports the audit-grade post-market surveillance that emerging regulations require.

The licensing position is component-level. Every device that integrates the continuity-identity IC infringes by integration; the licensing leverage applies to the chip vendor rather than to each end-product manufacturer. The patent positions the silicon-block embodiment at the layer where licensing economics produce maximum leverage.