Supply Chain Authentication Without PKI

by Nick Clark | Published March 27, 2026 | PDF

Supply chain authentication depends on PKI infrastructure that fragments at organizational boundaries. Each participant operates its own certificate authority or relies on a shared third party, creating trust relationships that are expensive to establish, brittle to maintain, and vulnerable to compromise at any certificate authority in the chain. Keyless identity enables authentication through accumulated behavioral continuity, eliminating the certificate infrastructure that supply chains cannot practically share.

The PKI problem across organizational boundaries

Public Key Infrastructure works well within a single organization. The organization operates a certificate authority, issues certificates to its devices and systems, and validates those certificates through a chain of trust rooted in its own CA. The problem arises when two organizations need to authenticate

each other's devices and data. Neither organization trusts the other's CA implicitly. Cross-certification is expensive and creates mutual dependency. Third-party CAs add cost and create single points of compromise.

In a supply chain with dozens of participants across multiple jurisdictions, the PKI problem becomes intractable. Each supplier, manufacturer, distributor, and retailer would need to establish certificate trust relationships with every other participant it interacts with. The number of trust relationships grows combinatorially. Certificate revocation must propagate across organizational boundaries in near real-time. A compromised CA anywhere in the chain can forge identities for any device certified by that CA.

The practical result is that most supply chains do not use cryptographic authentication at the device or entity level. They rely on network-level controls, bilateral contractual agreements, and manual verification processes that do not scale and cannot detect sophisticated counterfeiting or data manipulation.

Why blockchain and distributed ledger approaches fall short

Blockchain-based supply chain authentication records device identities and authentication events on a distributed ledger. This eliminates the single CA dependency but introduces a global consensus requirement. Every authentication event must be validated by the network, which imposes latency, transaction costs, and scalability limits that are incompatible with high-volume supply chain operations.

More fundamentally, blockchain authentication still depends on cryptographic keys. Each device has a private key that signs its identity claims. If the key is compromised, the identity is compromised. The blockchain records that a key signed something, not that the entity holding the key is the entity it claims to be. The key is the identity, and keys are stealable, copyable, and vulnerable to quantum attack.

How keyless identity addresses this

Keyless identity derives device and entity authentication from accumulated behavioral continuity rather than stored keys or certificates. A device's identity is its behavioral trajectory: the pattern of interactions, timing characteristics, operational parameters, and environmental signals that accumulate over the device's operational history.

Each interaction in the supply chain extends the device's hash chain with locally-sourced entropy. A sensor that has been reporting temperature readings for six months has an accumulated trust slope that cannot be forged by an attacker who does not have access to the actual device's operational history. The identity is not something the device possesses. It is something the device has become through its accumulated behavior.

Cross-organizational authentication does not require shared CAs, cross-certification, or third-party trust providers. When a device from one organization interacts with a system from another organization, the receiving system evaluates the device's trust slope: is this device's behavioral trajectory consistent with what it claims to be? The evaluation is local. No external authority must be consulted.

What implementation looks like

A supply chain deploying keyless authentication equips each device, whether a sensor, RFID reader, barcode scanner, or logistics controller, with trust slope generation capability. The device accumulates identity through its operational behavior. No enrollment step with a certificate authority is required.

When goods pass from one supply chain participant to another, the accompanying devices authenticate through trust slope validation rather than certificate exchange. The receiving participant evaluates whether the device's behavioral trajectory is consistent with its claimed identity and operational history. Counterfeited devices that lack genuine operational history fail this validation even if they carry cloned identifiers.

For pharmaceutical supply chains, keyless authentication provides a mechanism to detect counterfeit products at the device level. A genuine temperature-monitoring sensor that has been in continuous operation since the manufacturing stage has a trust slope that a replacement sensor, regardless of how perfectly it mimics the original's identifier, cannot replicate.

For regulatory compliance, the trust slope provides a continuous authentication record that demonstrates chain-of-custody integrity without depending on certificate infrastructure that could be compromised. The authentication is structural, post-quantum, and does not require trust in any external authority.

Keyless Identity All 21 steps →

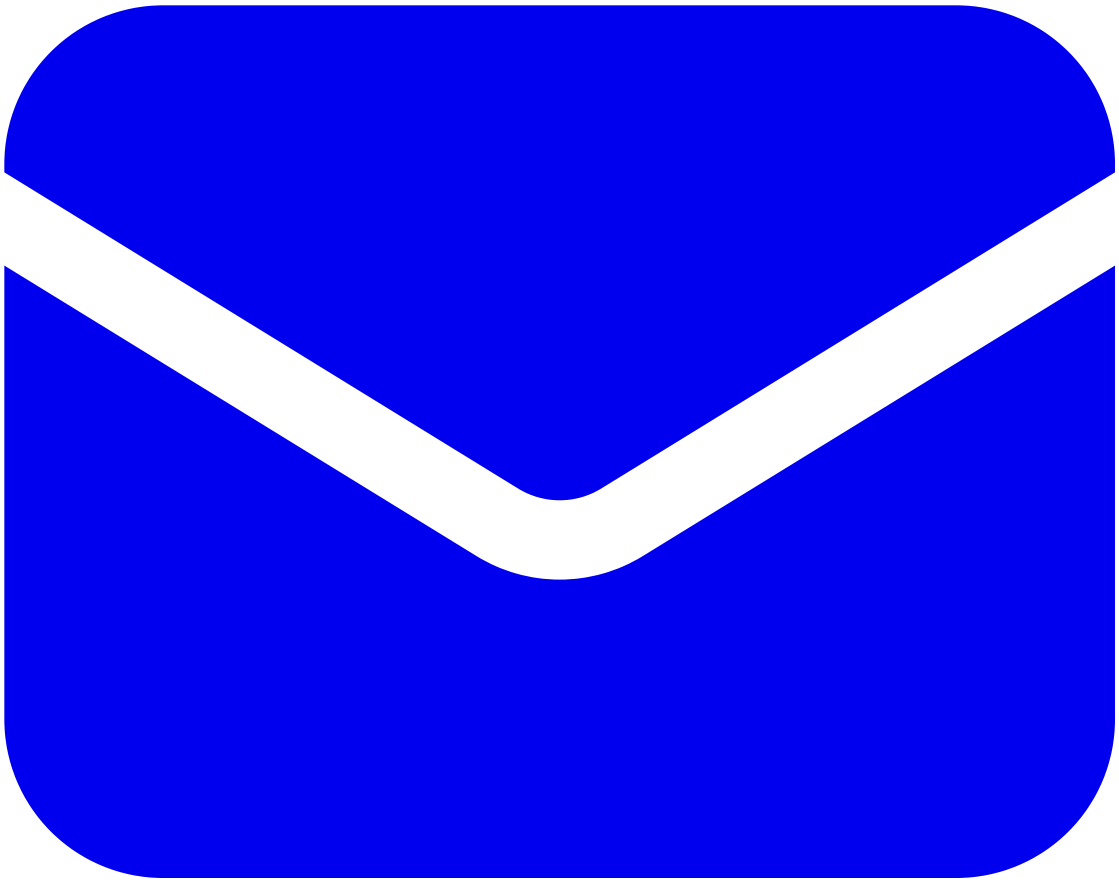
Identity from accumulated continuity. Post-quantum by construction.

Patent
US 19/388,580 · published
Primary Technical Disclosure
○ Stateless Device Pseudonymity and Secure Messaging in Cognition-Native Systems
Secondary Technical
○ Continuity-Based Biological Identity Using Trust-Slope Validation○ Trust Slope as Identity Primitive: Cumulative Hash Chains Replace Static Credentials○ Dual-Source Identity Derivation: Hardware Anchors and Local State Vectors Combined Per Epoch○ Stateless Symmetric Encryption: Session Keys Derived From Current Identity State○ Two-Stage Message Authentication: Transport Continuity Screening Before Semantic Validation○ Agent-Substrate Slope Entanglement: Binding Every Mutation Step to Its Execution Host○ Append-Only Mutation Lineage Log: Forward-Secure Identity Transition Chains○ Cumulative Slope Validation Across Substrates: Multi-Node Provenance Verification○ Quorum-Based Identity Recovery: Peer Attestation After Memory Loss○ Entropy Anchor Rotation: Proactive Identity Reseeding With Forward Links○ Biometric-Assisted Reseeding: Privacy-Preserving Fuzzy Extractors for Anchor Rotation○ Delayed Slope Validation: Bounded Proof Windows for Disconnected Environments○ Sparse Trust Slope Recovery: Compact Checkpoints for Resource-Constrained Devices○ Predictive Identity Validation: Drift Detection Before Full Discontinuity○ Legacy PKI Fallback: Session-Scoped Adapters With Strict Isolation Boundaries○ Post-Quantum Alignment: Hash-Based Security Without Vulnerable Hardness Assumptions
Applications (General)
○ Trust Slope Entanglement: Cryptographic Lineage for Semantic Agents○ Post-Quantum Enterprise Identity Migration○ Billions of IoT Devices Need Authentication Without Keys○ Financial Identity Without Credential Databases○ Patient Identity Through Behavioral Continuity● Supply Chain

Authentication Without PKI○ Smart Building Access Through Continuity○ Vehicle Operator Identity Binding○ Displaced Person Identity Without Documents
Applications (Specific)
○ Okta Centralized Enterprise Identity. The Keys That Prove It Are Still Stored Somewhere.○ Auth0 Made Developer Identity Easy. The Credential Model Underneath Did Not Change.○ YubiKey Made Hardware Authentication Practical. The Key Is Still the Vulnerability.○ CLEAR Made Airport Identity Fast. It Built a Biometric Database to Do It.○ Worldcoin Scans Irises to Prove Humanity. The Proof Depends on a Central Enrollment System.○ Jumio Automated ID Verification. The Verification Still Depends on Documents.○ Microsoft Entra Unified Cloud Identity. Identity Still Depends on Stored Credentials.○ Ping Identity Built Enterprise Federation. The Federation Depends on Shared Secrets.○ OneLogin Simplified Enterprise SSO. The SSO Token Is Still a Credential.○ Duo Security Made MFA Ubiquitous. The Second Factor Is Still a Credential.○ Thales HSMs Protect Key Material. The Keys Still Exist.○ Entrust Issues Digital Certificates. The Certificate Is a Stored Credential.○ DigiCert Secures the Web With TLS Certificates. The Certificate Model Has Structural Limits.○ Let's Encrypt Made TLS Free. The Certificate Model Is Still the Same.
Keyless Identity overview →
AQ
deterministic
autonomy

Legal

Last updated: 2026-03-03



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

Invented by Nick Clark | Founding Investors: Devin Wilkie