Smart Building Access Through Continuity

by Nick Clark | Published March 27, 2026 | PDF

Physical access control has not fundamentally changed in decades. Keys became cards, cards became fobs, fobs became phones, but the model remains the same: possess a credential, present it, gain access. Keyless identity replaces credential possession with behavioral continuity, where access derives from accumulated trust rather than something that can be copied, shared, or stolen. The door does not ask what you have. It evaluates who you have been.

The credential problem in physical access

Every physical access control system depends on credentials that can be transferred. A key can be copied. A card can be cloned. A PIN can be shared. A biometric template can be spoofed. Mobile credentials stored on phones are more convenient but inherit the vulnerabilities of the phone's security model. The credential is the identity, and credentials are inherently separable from the person they represent.

Building access management is operationally expensive because credentials must be issued, tracked, revoked, and replaced. When an employee leaves, their credentials must be deactivated across every access point. When a contractor needs temporary access, a credential must be provisioned and later revoked. When a credential is lost, every door it could access becomes a potential vulnerability until the credential is replaced and the lost one is deactivated.

Multi-tenant buildings face a compounded version of this problem. Each tenant manages its own access control for its spaces, but shared spaces like lobbies, parking structures, and conference facilities require cross-tenant credential management that no single tenant controls and no building management system handles gracefully.

Why biometric systems trade one vulnerability for another

Biometric access control, fingerprint readers, facial recognition, and iris scanners, eliminate the transferability of physical credentials but create stored biometric templates that present their own vulnerabilities. A stolen biometric template cannot be revoked because the biometric is the person. A spoofed fingerprint or a deepfake face can defeat systems that match against stored templates.

More fundamentally, biometric systems require enrollment: a point-in-time capture that creates the stored template. The system trusts the template because it was captured during a controlled enrollment process. But the ongoing relationship between the person and the template is based on static matching, not on behavioral continuity. A person who presented a valid fingerprint at enrollment is trusted every time that fingerprint matches, regardless of whether the person's behavior is consistent with their established pattern.

How keyless identity addresses this

Keyless identity derives access authorization from accumulated behavioral continuity. There is no credential to present, no template to match, and no enrollment event that creates a static reference. The person's identity is their accumulated trajectory of interactions with the building's systems: movement patterns, device associations, timing characteristics, and environmental signals.

The trust slope strengthens with each legitimate access event. A person who has been entering the building at consistent times, following consistent movement patterns, and interacting with building systems in consistent ways has a strong trust slope. An unauthorized person attempting to use the same access point has no accumulated trajectory and cannot forge one because each link in the chain depends on entropy sources specific to the actual person's interactions.

Access decisions are continuous rather than binary. Instead of a single credential check at the door, the system continuously evaluates the person's behavioral trajectory against their established pattern. Anomalous behavior, entering at an unusual time, accessing an unusual floor, or exhibiting movement patterns inconsistent with the established trajectory, triggers graduated responses rather than binary accept/reject.

What implementation looks like

A smart building deploying keyless access integrates trust slope evaluation into existing building infrastructure: elevator systems, door controllers, lighting systems, and HVAC zones. Each system contributes to and evaluates the occupant's behavioral trajectory. No separate access control hardware is required beyond the building systems that already exist.

For building operators, keyless access eliminates credential management overhead. No cards to issue, track, or revoke. When an employee leaves, their trust slope naturally decays through absence. No active deactivation is required. When a visitor arrives, their trust slope begins building from the moment they enter, providing graduated access that increases with legitimate presence.

For multi-tenant buildings, each tenant's space operates as a trust scope. The building's common areas have their own trust scope. Occupants build trust slopes within the scopes they legitimately use. Cross-tenant access is governed by the trust relationships between scopes, not by cross-tenant credential management.

For security teams, the continuous behavioral evaluation provides richer intelligence than binary access logs. Instead of knowing that a credential was presented at a door, the system provides a continuous behavioral assessment of every occupant, detecting anomalies that credential-based systems cannot identify.

Keyless Identity All 21 steps →

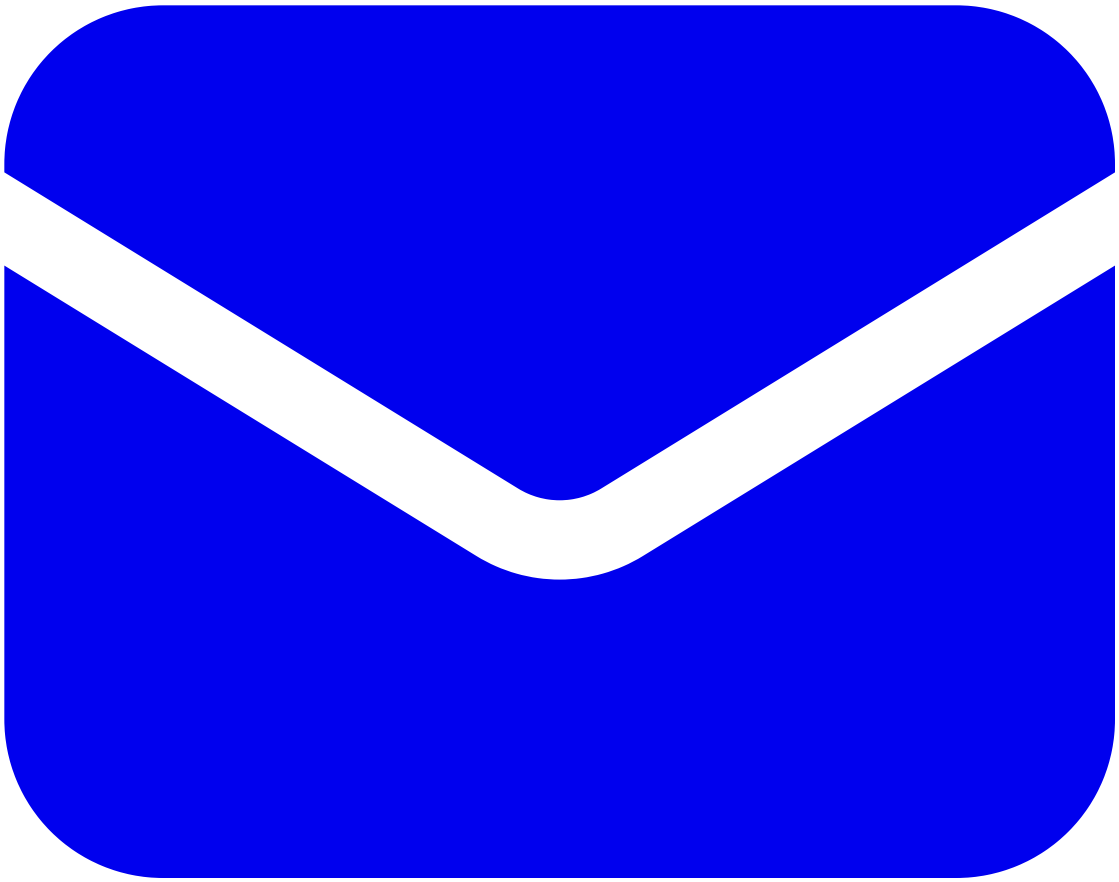
Identity from accumulated continuity. Post-quantum by construction.

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