Nick Clark · Published June 22, 2026 · PDF

When the Link Dies, the Identity Has to Live Onboard

In a contested radio environment, a drone swarm cannot reach a certificate authority, a token issuer, or its own command post. Yet drones still must prove identity to each other and validate that an incoming message is from a sibling, not an adversary spoofing one. Keyless hash-chain identity is the only architecture that holds.

The Condition: No Path to Any Authority

In a contested electromagnetic environment, a drone swarm operates under denial. The radio link to the operator is jammed or intermittent, satellite navigation is degraded or spoofed, and the path back to any command post is unreliable by design, because an adversary who can deny it will. Yet the drones still have to function as a swarm, and functioning as a swarm requires identity. Each drone must be able to prove to its siblings that it is a legitimate member, and each must be able to validate that an incoming instruction or observation actually came from a sibling rather than from an adversary spoofing one. This is the defense doctrine of denied, degraded, intermittent, and limited operations stated as an identity problem: identity has to work when there is no path to any authority that could vouch for it. The companion case essay, what drone jamming proves about trustworthy autonomy (/articles/what-drone-jamming-proves-about-trustworthy-autonomy), makes the operational argument; this article is the identity mechanism underneath it.

Why Every Stored-Secret Model Fails Here

Public-key infrastructure fails because it depends on reachability. Validating a certificate means checking it against an authority and, in practice, checking revocation, and a certificate authority that cannot be reached cannot be consulted; the swarm is left either trusting unvalidated certificates or refusing to operate. Pre-shared keys fail for the opposite reason: they are reachable but brittle. A symmetric key distributed across the swarm so that members can authenticate to each other is a single point of catastrophic failure, because the capture of one drone, an expected event in a contested environment, compromises the key and therefore every member that shares it. External attestation services fail for the same reason PKI does: if a drone proves its integrity by presenting an attestation from a cloud or platform provider, and that provider is unreachable, the proof cannot be produced. Every model that locates the proof of identity in a stored secret or an external issuer inherits a dependency that the contested environment is specifically designed to sever.

Why Keyless Continuity Holds

Keyless identity holds in this environment because the proof is carried, not fetched. A drone's identity is an append-only chain of dynamic hashes advanced by validated interaction, and its trust value is a computed property of that chain that any verifier can reconstruct by replaying it. A sibling validates an incoming message by checking that the sender's present chained state is the legitimate successor of states it has previously witnessed, locally, with no authority in the loop. There is no certificate to check against an unreachable registry and no shared secret whose capture unravels the swarm, because each drone's chain is its own and advances only through interactions it actually participated in.

Two further properties make this survivable under capture. Device entanglement binds the identity chain to the physical platform, so a chain cannot be lifted off a captured drone and replayed from adversary hardware; the proof is anchored in locally sourced

unpredictability that does not travel. Quorum recovery handles the temporary state loss that contested operation produces: a drone that loses connectivity or part of its state for a period can re-establish its standing through a threshold of peer validations rather than through a call home, so the swarm heals from within. Capture remains a real event with real consequences, but it is a contained, attributable one, the loss of one member, rather than a key disclosure that compromises the whole.

The General Point

The jamming case is the sharpest illustration of a general principle that the white paper Autonomy You Can Trust (/autonomy-you-can-trust) develops in full: when a system must act with no round-trip to authority, the things authority would have supplied, including identity, have to be carried inside the acting unit. PKI, pre-shared keys, and attestation services are all ways of supplying identity from outside, and outside is exactly what the adversary removes. Keyless continuity is identity that needs nothing it cannot carry, which is why it is the architecture that holds when the link dies.

Disclosure Scope

The keyless identity mechanism, including the append-only chain of validated dynamic hashes, the device entanglement that binds a chain to its physical platform, and the quorum recovery that re-establishes standing through peer validation rather than an issuer, is disclosed in the identity filing (U.S. Application No. 19/388,580, published as US 2026/0126730 A1), including its claims directed to entanglement. This article applies those disclosed mechanisms to the contested-link, denied-environment condition described in defense doctrine for denied, degraded, intermittent, and limited operations, and is the identity-mechanism companion to the case essay on drone jamming and to the autonomy white paper. References to operational doctrine are to public sources and are used for context only.

Keyless Identity (/keyless-identity)

All 36 steps → (/inventive-steps)

Identity from accumulated continuity. Post-quantum by construction.

PRIMARY TECHNICAL DISCLOSURE

- Stateless Device Pseudonymity and Secure Messaging in Cognition-Native Systems (/articles/stateless-device-pseudonymity-and-secure-messaging-in-cognition-native-systems)

SECONDARY TECHNICAL

- Continuity-Based Biological Identity Using Trust-Slope Validation (/articles/continuity-based-biological-identity-using-trust-slope-validation)
- Trust Slope as Identity Primitive: Cumulative Hash Chains Replace Static Credentials (/articles/keyless-identity/trust-slope-identity)
- Dual-Source Identity Derivation: Hardware Anchors and Local State Vectors Combined Per Epoch (/articles/keyless-identity/dual-source-derivation)
- Stateless Symmetric Encryption: Session Keys Derived From Current Identity State (/articles/keyless-identity/stateless-encryption)
- Two-Stage Message Authentication: Transport Continuity Screening Before Semantic Validation (/articles/keyless-identity/two-stage-auth)
- Agent-Substrate Slope Entanglement: Binding Every Mutation Step to Its Execution Host (/articles/keyless-identity/slope-entanglement)
- Append-Only Mutation Lineage Log: Forward-Secure Identity Transition Chains (/articles/keyless-identity/mutation-lineage-log)
- Cumulative Slope Validation Across Substrates: Multi-Node Provenance Verification (/articles/keyless-identity/cross-substrate-validation)
- Quorum-Based Identity Recovery: Peer Attestation After Memory Loss (/articles/keyless-identity/quorum-recovery)
- Entropy Anchor Rotation: Proactive Identity Reseeding With Forward Links (/articles/keyless-identity/anchor-rotation)
- Biometric-Assisted Reseeding: Privacy-Preserving Fuzzy Extractors for Anchor Rotation (/articles/keyless-identity/biometric-reseeding)
- Delayed Slope Validation: Bounded Proof Windows for Disconnected Environments (/articles/keyless-identity/delayed-validation)
- Sparse Trust Slope Recovery: Compact Checkpoints for Resource-Constrained Devices (/articles/keyless-identity/sparse-checkpoints)

- Predictive Identity Validation: Drift Detection Before Full Discontinuity (/articles/keyless-identity/predictive-drift)
- Legacy PKI Fallback: Session-Scoped Adapters With Strict Isolation Boundaries (/articles/keyless-identity/pki-fallback)
- Post-Quantum Alignment: Hash-Based Security Without Vulnerable Hardness Assumptions (/articles/keyless-identity/post-quantum)
- Continuity-Identity Processor IC: Silicon-Block Embodiment (/articles/keyless-identity/continuity-identity-processor-ic)
- Biological-Device Binding Through Continuity (/articles/keyless-identity/biological-device-binding)
- Multi-Modal Biometric Continuity Coupling (/articles/keyless-identity/multi-modal-continuity-coupling)

APPLICATIONS · GENERAL

- Trust Slope Entanglement: Cryptographic Lineage for Semantic Agents (/articles/keyless-identity/trust-slope-entanglement)
- Post-Quantum Enterprise Identity Migration (/articles/keyless-identity/post-quantum-migration)
- Billions of IoT Devices Need Authentication Without Keys (/articles/keyless-identity/iot-authentication)
- Financial Identity Without Credential Databases (/articles/keyless-identity/financial-identity-verification)
- Patient Identity Through Behavioral Continuity (/articles/keyless-identity/healthcare-patient-continuity)
- Supply Chain Authentication Without PKI (/articles/keyless-identity/supply-chain-authentication)
- Smart Building Access Through Continuity (/articles/keyless-identity/smart-building-access)
- Vehicle Operator Identity Binding (/articles/keyless-identity/vehicle-operator-identity)
- Displaced Person Identity Without Documents (/articles/keyless-identity/refugee-identity)
- Component-Level Identity Licensing at the Silicon Layer (/articles/keyless-identity/silicon-vendor-licensing)
- The Agent Identity Wave: Where the Whole Market Is Heading (/articles/keyless-identity/agent-identity-convergence)
- **When the Link Dies, the Identity Has to Live Onboard (/articles/keyless-identity/drone-swarm-jammed-identity)**
- Forced Off the Keys: Why the Post-Quantum Migration Points Past PKI to Keyless (/articles/keyless-identity/post-quantum-forcing-function)

APPLICATIONS · SPECIFIC

- Okta Centralized Enterprise Identity. The Keys That Prove It Are Still Stored Somewhere. (/articles/keyless-identity/okta)
- Auth0 Made Developer Identity Easy. The Credential Model Underneath Did Not Change. (/articles/keyless-identity/auth0)
- YubiKey Made Hardware Authentication Practical. The Key Is Still the Vulnerability. (/articles/keyless-identity/yubico)
- CLEAR Made Airport Identity Fast. It Built a Biometric Database to Do It. (/articles/keyless-identity/clear)
- Worldcoin Scans Irises to Prove Humanity. The Proof Depends on a Central Enrollment System. (/articles/keyless-identity/worldcoin)
- Jumio Automated ID Verification. The Verification Still Depends on Documents. (/articles/keyless-identity/jumio)
- Microsoft Entra Unified Cloud Identity. Identity Still Depends on Stored Credentials. (/articles/keyless-identity/microsoft-entra)
- Ping Identity Built Enterprise Federation. The Federation Depends on Shared Secrets. (/articles/keyless-identity/ping-identity)
- OneLogin Simplified Enterprise SSO. The SSO Token Is Still a Credential. (/articles/keyless-identity/onelogin)
- Duo Security Made MFA Ubiquitous. The Second Factor Is Still a Credential. (/articles/keyless-identity/duo-security)
- Thales HSMs Protect Key Material. The Keys Still Exist. (/articles/keyless-identity/thales-hsm)
- Entrust Issues Digital Certificates. The Certificate Is a Stored Credential. (/articles/keyless-identity/entrust)
- DigiCert Secures the Web With TLS Certificates. The Certificate Model Has Structural Limits. (/articles/keyless-identity/digicert)
- Let's Encrypt Made TLS Free. The Certificate Model Is Still the Same. (/articles/keyless-identity/lets-encrypt)
- Qorvo Secure Elements Authenticate, but Don't Track Continuity (/articles/keyless-identity/qorvo-secure-element)
- NXP Trust Anchor Stores Keys, Not Trust Slope (/articles/keyless-identity/nxp-trust-anchor)
- Infineon Secure Microcontrollers Need Continuity Logic On-Die (/articles/keyless-identity/infineon-secure-microcontroller)
- Microchip Trust Platform Fits Hardware, Misses Behavioral Continuity (/articles/keyless-identity/microchip-trust-platform)
- Indicio SSI Network and Anonyome Labs (/articles/keyless-identity/indicio-ssi)

- Sovrin Foundation Self-Sovereign Identity (/articles/keyless-identity/sovrin-foundation)
- W3C Decentralized Identifiers (DIDs) (/articles/keyless-identity/w3c-dids)
- W3C Verifiable Credentials (/articles/keyless-identity/w3c-verifiable-credentials)
- Keycard: Token-Issuer IAM Reaches Toward Identity Continuity (/articles/keyless-identity/keycard)
- Aembit: External Attestation Is Half the Answer (/articles/keyless-identity/aembit)
- Astrix Security: Discovery and Governance Without a Substrate (/articles/keyless-identity/astrix-security)
- Oasis Security: Non-Human Identity Governance, Externally Anchored (/articles/keyless-identity/oasis-security)
- Token Security: NHI Catalog Without Cryptographic Continuity (/articles/keyless-identity/token-security)
- Entro Security: Secret Discovery vs. Secret Elimination (/articles/keyless-identity/entro-security)

Keyless Identity overview → (/keyless-identity)