

Token Security: NHI Catalog Without Cryptographic Continuity

Token Security builds an authoritative, continuously maintained catalog of machine identities and their relationships, on the premise that an organization cannot secure what it cannot see. The catalog records what exists; its entries remain static credentials whose authenticity is a binary issued-or-revoked status, not a verifiable history.

Vendor and Product Reality

Token Security is a non-human identity security platform built around a machine-identity-first view of the enterprise. As publicly described, it discovers and catalogs the non-human identities across an organization, service accounts, tokens, keys, certificates, and the workloads and agents that use them, correlates each to its owner and its access, and continuously assesses exposure so that risky or orphaned identities can be remediated. Its emphasis is the catalog: a single, continuously maintained inventory of machine identities and their relationships, on the premise that an organization cannot secure what it cannot see. Given how fragmented machine-identity data is across cloud and SaaS, an authoritative catalog is a real and valuable thing to build.

The Architectural Choice: A Catalog Without Continuity

Token Security catalogs identities; it does not give them cryptographic continuity. The entries in the catalog are existing credentials, secrets and keys and tokens, each a static artifact whose validity is a matter of whether it has been issued and not yet revoked. The catalog records what exists and how risky it is, but each cataloged identity remains a thing that can be copied, replayed, or stolen, and whose authenticity is a binary issued-or-revoked status rather than a verifiable history. There is no notion, in a catalog of static credentials, of an identity proving that its present state is the legitimate successor of its past, because the credentials it catalogs have no such state to advance. Visibility into a population of replayable secrets is necessary, but it is a different thing from making the secrets non-replayable.

What the Keyless Primitive Provides

Keyless identity gives each identity the cryptographic continuity a catalog of static credentials cannot. Identity is an append-only chain of validated dynamic hashes, so authenticity is not a binary issued-or-revoked flag but a verifiable history: a principal proves it is itself by demonstrating that its present chained state legitimately follows from states a verifier has witnessed. Such an identity cannot be replayed from a captured artifact, because there is no artifact to capture, and it is entangled to its device so it cannot be lifted. A catalog of keyless identities records continuity rather than credentials, and risk assessment over it asks whether a chain's history is coherent rather than whether a secret has leaked. Cataloging remains useful; what it catalogs becomes identities that carry their own proof.

Category Convergence

Token Security confirms that the enterprise needs an authoritative, continuously maintained view of machine identity. The keyless primitive ensures that the identities being cataloged are themselves non-replayable and self-proving, so that visibility is

over continuity rather than over a sprawl of static secrets. The two compose: maintain the catalog, and migrate the cataloged identities toward computed continuity so that what is inventoried cannot be stolen and reused. No relationship, endorsement, or infringement is asserted; the comparison is architectural.

Disclosure Scope

The keyless identity mechanism, in which identity is a validated, append-only chain of dynamic hashes that proves itself by verifiable continuity rather than by a static, replayable credential, and which is device-entangled, is disclosed in the identity filing (U.S. Application No. 19/388,580, published as US 2026/0126730 A1). This article compares that disclosed mechanism with Token Security's publicly described machine-identity catalog and positions cryptographic continuity as what a catalog of static credentials lacks. References to Token Security are to public materials and are used for comparison only.

Keyless Identity (</keyless-identity>)

[All 36 steps → \(/inventive-steps\)](/inventive-steps)

Identity from accumulated continuity. Post-quantum by construction.

PRIMARY TECHNICAL DISCLOSURE

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

SECONDARY TECHNICAL

- [Continuity-Based Biological Identity Using Trust-Slope Validation \(/articles/continuity-based-biological-identity-using-trust-slope-validation\)](/articles/continuity-based-biological-identity-using-trust-slope-validation).
- [Trust Slope as Identity Primitive: Cumulative Hash Chains Replace Static Credentials \(/articles/keyless-identity/trust-slope-identity\)](/articles/keyless-identity/trust-slope-identity).

- [Dual-Source Identity Derivation: Hardware Anchors and Local State Vectors Combined Per Epoch \(/articles/keyless-identity/dual-source-derivation\)](/articles/keyless-identity/dual-source-derivation)
- [Stateless Symmetric Encryption: Session Keys Derived From Current Identity State \(/articles/keyless-identity/stateless-encryption\)](/articles/keyless-identity/stateless-encryption)
- [Two-Stage Message Authentication: Transport Continuity Screening Before Semantic Validation \(/articles/keyless-identity/two-stage-auth\)](/articles/keyless-identity/two-stage-auth)
- [Agent-Substrate Slope Entanglement: Binding Every Mutation Step to Its Execution Host \(/articles/keyless-identity/slope-entanglement\)](/articles/keyless-identity/slope-entanglement)
- [Append-Only Mutation Lineage Log: Forward-Secure Identity Transition Chains \(/articles/keyless-identity/mutation-lineage-log\)](/articles/keyless-identity/mutation-lineage-log)
- [Cumulative Slope Validation Across Substrates: Multi-Node Provenance Verification \(/articles/keyless-identity/cross-substrate-validation\)](/articles/keyless-identity/cross-substrate-validation)
- [Quorum-Based Identity Recovery: Peer Attestation After Memory Loss \(/articles/keyless-identity/quorum-recovery\)](/articles/keyless-identity/quorum-recovery)
- [Entropy Anchor Rotation: Proactive Identity Reseeding With Forward Links \(/articles/keyless-identity/anchor-rotation\)](/articles/keyless-identity/anchor-rotation)
- [Biometric-Assisted Reseeding: Privacy-Preserving Fuzzy Extractors for Anchor Rotation \(/articles/keyless-identity/biometric-reseeding\)](/articles/keyless-identity/biometric-reseeding)
- [Delayed Slope Validation: Bounded Proof Windows for Disconnected Environments \(/articles/keyless-identity/delayed-validation\)](/articles/keyless-identity/delayed-validation)
- [Sparse Trust Slope Recovery: Compact Checkpoints for Resource-Constrained Devices \(/articles/keyless-identity/sparse-checkpoints\)](/articles/keyless-identity/sparse-checkpoints)
- [Predictive Identity Validation: Drift Detection Before Full Discontinuity \(/articles/keyless-identity/predictive-drift\)](/articles/keyless-identity/predictive-drift)
- [Legacy PKI Fallback: Session-Scoped Adapters With Strict Isolation Boundaries \(/articles/keyless-identity/pki-fallback\)](/articles/keyless-identity/pki-fallback)
- [Post-Quantum Alignment: Hash-Based Security Without Vulnerable Hardness Assumptions \(/articles/keyless-identity/post-quantum\)](/articles/keyless-identity/post-quantum)
- [Continuity-Identity Processor IC: Silicon-Block Embodiment \(/articles/keyless-identity/continuity-identity-processor-ic\)](/articles/keyless-identity/continuity-identity-processor-ic)
- [Biological-Device Binding Through Continuity \(/articles/keyless-identity/biological-device-binding\)](/articles/keyless-identity/biological-device-binding)
- [Multi-Modal Biometric Continuity Coupling \(/articles/keyless-identity/multi-modal-continuity-coupling\)](/articles/keyless-identity/multi-modal-continuity-coupling)

APPLICATIONS · GENERAL

- [Trust Slope Entanglement: Cryptographic Lineage for Semantic Agents \(/articles/keyless-identity/trust-slope-entanglement\)](/articles/keyless-identity/trust-slope-entanglement)

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

APPLICATIONS · SPECIFIC

- [Okta Centralized Enterprise Identity. The Keys That Prove It Are Still Stored Somewhere. \(/articles/keyless-identity/okta\)](/articles/keyless-identity/okta).
- [Auth0 Made Developer Identity Easy. The Credential Model Underneath Did Not Change. \(/articles/keyless-identity/auth0\)](/articles/keyless-identity/auth0)
- [YubiKey Made Hardware Authentication Practical. The Key Is Still the Vulnerability. \(/articles/keyless-identity/yubico\)](/articles/keyless-identity/yubico).
- [CLEAR Made Airport Identity Fast. It Built a Biometric Database to Do It. \(/articles/keyless-identity/clear\)](/articles/keyless-identity/clear)
- [Worldcoin Scans Irises to Prove Humanity. The Proof Depends on a Central Enrollment System. \(/articles/keyless-identity/worldcoin\)](/articles/keyless-identity/worldcoin).
- [Jumio Automated ID Verification. The Verification Still Depends on Documents. \(/articles/keyless-identity/jumio\)](/articles/keyless-identity/jumio)
- [Microsoft Entra Unified Cloud Identity. Identity Still Depends on Stored Credentials. \(/articles/keyless-identity/microsoft-entra\)](/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 Anonymome 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](#))