Nick Clark · Published June 22, 2026 · PDF

Oasis Security: Non-Human Identity Governance, Externally Anchored

Oasis brings non-human identities under governed lifecycle management, from provisioning through rotation to decommissioning, with the ownership and review discipline human identities receive. The lifecycle is genuine, but the trust it manages is anchored outside the identity, conferred and renewed by external infrastructure.

Vendor and Product Reality

Oasis Security is a non-human identity management platform that has raised substantial venture funding, including a reported Series B in the nine-figure range, reflecting how quickly the category has matured. As publicly described, Oasis discovers an organization's non-human identities across cloud and SaaS, builds an inventory with ownership and usage context, assesses their risk and posture, and manages their lifecycle, from provisioning through rotation to decommissioning. Where some tools emphasize detection, Oasis emphasizes governed lifecycle management: bringing non-human identities under the same kind of ownership, review, and offboarding discipline that human identities receive. It is a mature answer to a real operational problem.

The Architectural Choice: Externally Anchored Lifecycle

Oasis manages the lifecycle of identities whose trust is anchored outside themselves. The non-human identities it governs are issued and validated by existing infrastructure, cloud IAM, secrets managers, identity providers, and Oasis orchestrates their creation, rotation, and retirement against that infrastructure. The lifecycle discipline is genuine, but the anchor of trust remains external: each identity is trustworthy because an issuer says so, and its continuity across rotations is continuity that the management plane maintains by re-issuing and re-binding credentials. The identity does not carry its own proof; it is a managed record whose authority is conferred and renewed from outside. Lifecycle management makes that external anchoring orderly; it does not move the anchor into the identity.

What the Keyless Primitive Provides

Keyless identity anchors trust inside the identity itself. Standing is a computed property of an append-only chain advanced by validated interaction, so continuity across time is intrinsic rather than maintained by a management plane re-issuing credentials. Rotation, in the conventional sense of replacing a secret before it is compromised, has no analog to perform, because there is no static secret with a compromise window; the chain simply advances. Provisioning is the genesis of a chain rather than the minting of a credential, and decommissioning is decay, the structural return to baseline when an identity is no longer exercised. The lifecycle Oasis orchestrates externally becomes, for a keyless identity, a property of the construction. Governance and ownership context remain valuable, but the trust they govern is carried by the identity rather than conferred upon it.

Category Convergence

Oasis demonstrates that the market wants non-human identity managed with real lifecycle rigor, not merely detected. The keyless primitive supplies identities whose lifecycle is largely intrinsic, shrinking the external machinery required to keep them trustworthy over time. An organization can apply Oasis-style governance to its existing estate while migrating critical identities to computed continuity, so that ownership and review remain while rotation and re-issuance fall away. 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 whose trust value is computed and whose continuity, renewal, and decay are intrinsic to the construction rather than maintained by an external management plane, 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 Oasis Security's publicly described non-human-identity lifecycle management and positions the keyless primitive as anchoring trust inside the identity. References to Oasis are to public materials and are used for comparison 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)