Nick Clark · Published June 22, 2026 · PDF

Aembit: External Attestation Is Half the Answer

Aembit gives workloads and agents managed identity and brokers their access without stored secrets, verifying each request through attestation drawn from the surrounding platform. It removes the stored secret and replaces it with a live external check. That is half the answer; the other half is an identity the principal carries.

Vendor and Product Reality

Aembit is a workload identity and access management platform. As publicly described, it gives a workload, a service, a script, or increasingly an agent, a managed identity and brokers its access to other services without embedding a static secret in the workload. Rather than storing an API key or password, the workload requests access at runtime, Aembit verifies the workload's identity and the conditions of the request, and a short-lived credential is issued for that specific access. The verification draws on attestation: signals about where and how the workload is running, often sourced from the surrounding platform such as a cloud provider's instance identity or an orchestrator's metadata. The product replaces long-lived secrets with policy-governed, attested, just-in-time access, which is a substantial improvement over the status quo of secrets sprawl.

The Architectural Choice: External Attestation

Aembit's identity assurance rests on attestation from an external trust provider. The workload is trusted because the cloud or orchestration platform vouches that it is what it claims to be, and Aembit binds access decisions to that vouching. This is the right instinct, and it is half the answer: it removes the stored secret as the thing being proved and replaces it with a live, contextual check. But it relocates the dependency rather than dissolving it. The identity is only as available and as trustworthy as the external attestor, and the chain of trust terminates in that provider's signing infrastructure and its reachability. In an environment where the attestor cannot be reached, or for a principal that does not run inside a platform willing to attest for it, the model has nothing underneath to fall back on. Attestation answers is this workload running where it should; it does not give the workload an identity it carries independently of the platform attesting for it.

What the Keyless Primitive Provides

Keyless identity supplies the other half: an identity the principal carries and computes from its own validated history, requiring no external attestor in the loop at the moment of proof. Identity is an append-only chain of dynamic hashes advanced by validated interaction, with a trust value reconstructed by replaying the chain, entangled to the device so it cannot be lifted, and recoverable through peer quorum. A verifier confirms continuity directly against the principal's chain rather than against a third party's attestation, so the proof holds when the attestor is unreachable and applies to principals that no platform attests for. External attestation and computed continuity are not exclusive; the strongest posture composes them, using platform attestation where it is available and falling back on carried continuity where it is not, with the keyless chain as the floor rather than the gap.

Category Convergence

Aembit confirms the direction: secretless, attested, just-in-time access is where workload and agent identity are heading, and Aembit is a mature expression of it. The keyless primitive extends that direction past the external attestor to identity the principal holds on its own. The two compose cleanly: keyless continuity can serve as the carried floor beneath an attestation-brokered access layer, so that access survives the loss of the attestor rather than failing closed on its absence. 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 with a computed trust value, device entanglement, and quorum recovery, requiring neither a certificate authority nor an external attestor at the moment of proof, 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 Aembit's publicly described attestation-brokered workload IAM and positions carried continuity as the complement to external attestation. References to Aembit 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)