Nick Clark · Published June 22, 2026 · PDF

Keycard: Token-Issuer IAM Reaches Toward Identity Continuity

Keycard builds identity and access management specifically for AI agents, issuing scoped, short-lived credentials with policy and audit. It reaches toward identity continuity more than most. The question is where that continuity is anchored: in an issuer, or in the agent's own validated history.

Vendor and Product Reality

Keycard is a recent, well-funded entrant building identity and access management specifically for AI agents rather than for human users or traditional workloads. As publicly described, its approach treats an agent as a first-class principal that is issued scoped, short-lived credentials to act on a user's or organization's behalf, with policy controlling what each agent is permitted to do and an audit trail of agent actions. The framing is current and correct about the problem: an agent that acts autonomously needs an identity distinct from the human who launched it and from the service it calls, and the static API keys and shared service accounts that agents are improvised onto today are a liability. Keycard is part of the wave of capital and engineering that formed around this realization, and on its own terms it is a real product addressing a real gap.

It also reaches, more than most, toward identity continuity rather than mere credential issuance, which is what makes it worth examining closely. The question is where the continuity is anchored.

The Architectural Choice: A Token Issuer

At the cryptographic layer, Keycard's model is issuer-based. An authority mints a token that an agent presents, and a relying party trusts the token because it trusts the issuer. Scoping the token narrowly and shortening its lifetime are genuine improvements over a static key, and policy over agent behavior is valuable, but the identity primitive underneath remains a credential handed down by an issuer. The agent's ability to prove who it is depends on the issuer being reachable to mint and on the relying party trusting that issuer's signature, and the continuity the product reaches toward is continuity the issuer maintains on the agent's behalf rather than continuity the agent computes from its own activity. Remove the issuer from the loop, or compromise the issuing key, and the identity has nothing of its own to fall back on.

What the Keyless Primitive Provides

Keyless identity removes the issuer entirely. An agent's identity is an append-only chain of dynamic hashes advanced only by independently validated interaction, and its standing is a trust value that any verifier reconstructs by replaying the chain. No authority mints the credential, because the credential is computed from the agent's own validated history; no relying party holds or trusts an issuer's signing key, because it validates that the agent's present chained state is the legitimate successor of states it has witnessed. The continuity that Keycard maintains for the agent through an issuer is, in the keyless model, intrinsic to the agent: it is the agent's own chain, entangled to its hardware so it cannot be lifted, recoverable through peer quorum rather than re-issuance. The result is identity that survives the issuer being unreachable and has no issuing key whose compromise yields impersonation.

Category Convergence

Keycard is evidence for the thesis, not a target of it. That a credibly funded team is building agent identity around scoped, short-lived, continuity-seeking credentials confirms that the market is moving in the keyless direction: away from static secrets, toward dynamic and earned identity. Keycard advances along that axis and stops at the issuer; the keyless primitive is the same axis taken to its end, where there is no issuer left. The two are complementary in posture: a deployment can adopt issuer-based agent IAM today and migrate the identity primitive underneath it toward computed continuity as the keyless model is adopted, without changing the policy and audit layers built on top. 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, and which requires neither a certificate authority nor a credential issuer, 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 Keycard's publicly described issuer-based agent IAM and positions the keyless primitive as the issuer-free endpoint of the same convergence. References to Keycard are to public materials and are used for comparison only.

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)