Nick Clark · Published June 22, 2026 · PDF

The Agent Identity Wave: Where the Whole Market Is Heading

In late 2024, agent identity was a research term. A year later it was among the most heavily funded categories in enterprise security. Look at where every credible vendor now points: away from static secrets, away from central issuers, away from PKI. They are converging on the same architecture from different starting points.

From Research Term to Funded Category

In late 2024, agent identity was a phrase in research papers. Within roughly a year it had become one of the most heavily funded and consolidated categories in enterprise security. The shape of the activity is unmistakable even before the dollar figures: established identity and security vendors acquiring agent-identity and non-human-identity startups, hyperscalers shipping dedicated agent-identity features into their directories, and standards bodies opening working groups specifically for agentic and non-human identity. The market decided, almost at once, that the identity model built for human users logging into applications does not extend to autonomous software acting on its own, and it began buying and building toward something else.

What that something else is, exactly, is the interesting part. Look past the branding and the credible vendors are converging, from different starting points, on the same set of properties: identity that is dynamic rather than enrolled once, scoped narrowly rather

than granted broadly, and free of long-lived static secrets. They are feeling their way toward a destination none of them has fully reached.

Two Intermediate Stops the Market Has Settled On

Two mainstream approaches dominate the current agent-identity conversation, and both are intermediate stops rather than destinations. The first is decentralized identifiers paired with verifiable credentials. This model improves on centralized directories by letting a subject present cryptographically verifiable claims without a single authority brokering every transaction, and it is the direction the standards work leans. But it remains key-based: a decentralized identifier resolves to a document containing public keys, and the subject proves control by signing with the corresponding private key. The static secret has been relocated, not removed, and the post-quantum migration that threatens every classical signature threatens this model with it.

The second is non-human identity and token-scoping. This model treats each workload, service, and agent as a first-class identity that is issued short-lived, narrowly scoped credentials, often attested by the surrounding platform such as a cloud metadata service or a Kubernetes control plane. It is a real improvement: short-lived beats long-lived, scoped beats broad, attested beats self-asserted. But it remains issuer-based. Some authority, the cloud provider, the orchestrator, the secrets manager, mints the credential, and the agent's identity is only as available and as trustworthy as that issuer. Remove the issuer's reach, as a contested or disconnected environment does, and the identity has nothing to stand on.

The Destination the Convergence Implies

Both stops are steps along a single axis: away from static secrets, away from central authorities, toward identity that an agent can prove from its own ongoing activity. The endpoint of that axis is identity with no certificate authority and no issuer at all, where

the credential is not stored or minted but computed. The keyless mechanism described across this body of work is that endpoint. Identity is an append-only chain of dynamic hashes advanced only by independently validated interaction, with a trust value that is a computed property of the chain rather than a stored score, entangled to the device so it cannot be lifted, and recoverable through a quorum of peers rather than through an issuer. There is no enrollment record whose compromise yields impersonation, because there is no static secret whose disclosure replays as authentication, and there is no issuer whose unreachability suspends the identity, because the proof is continuity the agent carries.

This is what the decentralized-identifier camp approximates without leaving keys behind, and what the non-human-identity camp approximates without leaving the issuer behind. The market is converging on a destination it has not named; the keyless primitive names it.

Timing and the Standards Pull

The convergence is also visible in the standards bodies. Working groups have formed specifically around identity management for agentic systems and open agent identity, and industry security alliances have begun publishing guidance on identity and access management for autonomous agents. The direction of all of this work is the same one the vendors are moving in: dynamic, scoped, attestable, less dependent on stored secrets. The keyless mechanism's priority predates the wave, with a filing date in late 2024 ahead of the consolidation and the standards activity that followed, which positions it not as a late entrant chasing the category but as a prior articulation of the destination the category is migrating toward. The point of this article is not that any particular vendor infringes; it is that an entire market, independently and from many directions, is walking toward an architecture that the keyless primitive already describes in full.

Disclosure Scope

The keyless identity mechanism described here, in which identity is a validated, append-only chain of dynamic hashes with a computed trust value, device entanglement, and quorum recovery, and which depends on 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 situates that disclosed mechanism against the publicly reported convergence in the agent-identity market and the direction of the relevant standards work, and argues that the market's intermediate models, key-based decentralized identifiers and issuer-based non-human identity, are steps toward the keyless destination the filing describes. References to specific vendors, acquisitions, and standards efforts are to public reporting and published materials and are used for context only; no relationship, endorsement, or infringement is asserted.

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)