Nick Clark · Published July 30, 2026 · PDF

When the Credential Is Stolen and Still Valid

When a platform security lead finds that a service credential issued to one of her long-lived agents has been copied, the discovery reaches her as an absence rather than an alarm: a log full of successful authentications, none of which she can attribute to a particular holder. Rotating the secret closes the window going forward and leaves the preceding weeks unattributable, because her records captured presentation rather than continuity. This article describes that failure inside one deployment, then describes what United States Patent Application 19/388,580 discloses in response: identity expressed as a trust slope, a cumulatively validated sequence of dynamic hashes, where acceptance turns on whether a presented successor is a valid descendant of a previously trusted state under policy-bounded checks.

The Tuesday the Log Agreed With the Attacker

The platform security lead at a mid-size freight brokerage keeps about four hundred autonomous agents in production. They negotiate capacity against carrier APIs, reconcile rate confirmations, and hold open long-running jobs on edge nodes at three terminals that lose connectivity for hours at a stretch. Each agent carries a scoped service credential minted at deploy time and rotated on a ninety-day cadence.

At 6:40 on a Tuesday morning she is looking at a dashboard for an unrelated reason and notices that an agent assigned to a lane that closed in May has been authenticating steadily. She pulls the access records. Every request from that agent identifier was accepted. Every one of them passed the check her gateway performs, because the check her gateway performs is whether the presented secret matches the secret on file, and it does.

She spends the next hour on a question her deployment was not built to answer. Not "was this credential valid," which the log already tells her nine thousand times over, but which of those nine thousand requests her agent actually made, and which were made by whatever else holds a copy of the same string. Her gateway wrote down that a valid credential was presented. It did not write down anything that would distinguish one holder of that credential from another, because in her setup the credential is the same object in both hands and produces the same evidence in both.

By 8:00 she has rotated the secret and killed the agent. That is the last decisive thing she can do that morning.

What She Cannot Reconstruct

Her rotation ended the exposure. It did not touch her record.

Her problem is that seven weeks of accepted activity are now unattributable, and no amount of subsequent investigation makes them attributable, because the distinguishing information was never captured in the first place. This is not a retention gap she can close by turning up log verbosity next quarter. Her gateway recorded that a match occurred. That match is all her record holds.

Those consequences are already downstream and already acted upon. Rate confirmations issued under those sessions went to carriers who dispatched trucks. Counterparties reconciled against them. Her brokerage's own ledger treats those

bookings as authorized, because in her deployment authenticated and authorized are recorded by the same event. When her general counsel asks which commitments the company actually made, she can state which requests authenticated. She cannot state which her agent originated. In a business where that answer decides who eats a cancellation, the gap is the whole question.

She also loses something quieter. Her incident timeline has no start. She can bound the exposure only by the credential's issue date, because there is no point in her records where the behavior of the holder changed in a way her gateway would have noticed. Seven weeks is not her estimate of the compromise. Seven weeks is the age of the secret, which is the only bound she has left.

The credential was stolen once. Her evidentiary loss is permanent, and permanent for a structural reason rather than an operational one: her deployment produced identical evidence for two different holders, so her evidence cannot later be separated into two piles.

Why Her Revocation Arrives After the Fact

Her credential is a bearer object. Whatever presents it is treated by her gateway as the agent it was issued to, which means possession and identity are the same fact for her purposes. Nothing about the second holder is anomalous under her checks, because her checks ask only whether the secret is right.

Were her agents short-lived, she could shorten the rotation window until the exposure was small enough to accept. They are not. Her terminal nodes run jobs that survive disconnection for hours, and a rotation cadence tight enough to bound the damage would break the jobs that make the deployment worth having. Her ninety days is not laziness. It is the setting that keeps her fleet running, and it is also the setting that sized her loss.

Were her gateway able to bind an accepted request to something the second holder does not have, she would have a discriminator. As her runtime is configured today, the only thing bound into the request is the secret itself, and the secret travels. Copying it costs the attacker nothing and leaves her nothing.

She could add central attestation, and for her deployment that trades one exposure for another: her terminal nodes are exactly the ones that cannot reach a central authority when they most need to authenticate, and a check that fails open under disconnection is not a check she can rely on for those nodes.

The pattern underneath all four of these, in her case, is that her identity evidence is static while the thing she wants to detect is a change of holder. She is asking a value that never varies to tell her that something varied.

Identity as a Sequence Rather Than a Secret

United States Patent Application 19/388,580 discloses a memory-native identity substrate in which a device or agent expresses identity as a trust slope, described in the specification as the cumulatively validated sequence of Dynamic Agent Hashes (DAHs) or Dynamic Device Hashes (DDHs) formed by successive, verifiable identity mutations, rather than as a static credential. Trust-slope continuity, as the specification defines it, denotes that a presented successor is a valid descendant of a previously trusted state under policy-bounded checks.

A slope root 101 is established at initialization. In one disclosed embodiment, a static hardware anchor 108 such as a TPM, TEE, or SoC identifier is combined with a volatile salt 109. In another, locally observed signals are collected into a local state vector 105, processed by an extractor 106 into a bounded pseudorandom token 107, and combined with the volatile salt. A semantic context vector 110 and a memory state indicator 111 may be incorporated to bind role, zone, or process mix into the initial identity. A hybrid embodiment hashes both sources into the same step.

An update rule 112 advances the identity by concatenating the prior hash with a fresh entropy input and a domain-separating tag. The specification gives DAH_t = H(DAH_{t-1} ∥ Ext(X_t) ∥ salt_t ∥ tag) for the local-state embodiment and DAH_t = H(DAH_{t-1} ∥ KDF(HWID, salt_t) ∥ tag) for the hardware-anchor embodiment, producing successive identities DAH_1 120, DAH_2 130, and DAH_3 140 along a verifiable trust slope 150. Each step records a mutation class 160 identifying the semantic reason for the step, such as role update, delegation, or policy commit.

The specification states that a DAH or DDH is ephemeral, computed per step, and never reused as a standing credential, and that observation or disclosure of any single DAH or DDH does not enable impersonation because acceptance requires monotonic progression from a prior trusted state under the published update rule and policy-bounded continuity checks. In the disclosed validation process 500, a node receiving a claimed identity DAH_x 510 performs a fast continuity comparison 520 against its last trusted value; a claim satisfying continuity is classified in-slope 530, and one that does not is classified off-slope 540 and treated as a probable spoof or forgery. Replay resistance is described as binding acceptance to monotonic progression and enforcing non-reuse of previously accepted successors within a policy horizon, with presentations that equal a previously accepted value or regress behind the stored reference rejected. Failure outcomes 545 are recorded with explicit reasons 550 such as continuity violation, neighborhood mismatch, salt staleness, cadence anomaly, or replay detection, and local policy may reject, degrade the sender's trust score 480, or quarantine the sender 490.

Message handling composes with this. In process 400 a sender derives a symmetric key from the recipient's current DDH or DAH and a domain-separating context 402, embeds a contemporaneously computed copy of its own DAH inside the ciphertext 403, and places its current DAH in the transport header 405. The receiver screens the header for continuity before decrypting, derives its key from its own current identity, and then compares the embedded sender DAH 440 against the expected successor on the sender's stored slope before acceptance 450.

For agent mutation, the disclosure describes substrate entanglement: each agent-side transition is bound to the executing host's device identity through a host-signed trace, and the specification describes a verifying node failing closed where a trace entry's host signature is invalid or the entry does not open to the host identity. Lineage is described as append-only, each entry folded into a cumulative chain with periodic anchors, so that in that arrangement omission, reordering, or modification of an entry diverges the terminal value and fails opening against the last anchor. Sparse checkpoints and bounded proof windows are disclosed for verifiers holding limited state, alongside anchor rotation with forward links and quorum-based recovery from previously trusted peers.

Where the disclosure quantifies strength, it does so conditionally. Letting λ denote the min-entropy in bits of the per-step unpredictability contribution after extraction, the specification puts offline next-step forgery at a success probability of approximately 2^{-λ}, and approximately 2^{-λ/2} under quantum amplitude-amplification search, with 256 to 512 bit extractor outputs and digests described as providing conservative margins.

Where This Leaves Her Deployment

Several things the security lead needs sit outside what the disclosed architecture speaks to.

It does not give her back the seven weeks. Nothing in a forward-looking identity construction reconstructs evidence her gateway never wrote.

For her terminal nodes, the strength of continuity checking is conditioned on inputs the attacker does not hold. The specification frames its resistance in exactly those terms, stating that an attacker lacking the device's local state or volatile salt cannot feasibly

synthesize valid successors. An adversary who has taken her host itself, and with it the local state that host observes, is a different problem from the copied string she found on Tuesday, and she would need to size that separately.

Continuity also speaks to descent, not to judgment. Were her fleet running on this substrate, an in-slope successor would tell her the step is a valid descendant of a state she previously trusted. It would not tell her the booking was a good booking. Policy correctness for her lanes stays hers, and the mutation classes recorded per step describe the semantic reason for a step rather than evaluate it.

Her carrier APIs are another matter. The disclosure confines fallback identifiers and PKI signatures to a segregated adapter whose materials are never hashed into DAH or DDH updates, so on her legacy integrations she would get whatever her adapter is configured to accept, not what the slope provides.

Her intermittently connected terminals would carry an operational cost as well. The specification describes senders encrypting under a stale recipient identity and recovering through a bounded rekey failure rate, a short challenge-response rekey handshake, or a checkpoint request, and describes receivers implementing a two-epoch acceptance window with per-sender rate limits. Tuning that for nodes offline for hours would be her work, and the checkpoint cadence she picks trades storage against replay effort by the specification's own account.

Finally, the quantified margins above depend on λ, the min-entropy of her per-step contribution. That is a parameter of her deployment, not something she inherits for free.

Disclosure Scope

This article describes subject matter disclosed in United States Patent Application 19/388,580, titled "Systems and Methods for Memory-Native Identity and Authentication." It is written for practitioners.

Nothing here characterizes the scope of any claim, pending or issued, or should be read as limiting, disclaiming, or defining any claim term. The mechanisms described are embodiments disclosed in the application, and reference to particular embodiments does not indicate that others are excluded. Nothing here constitutes an admission regarding the state of the art, the content or scope of any prior art, or the patentability of any subject matter. The scenario is illustrative and depicts no actual person, company, product, or incident.

Keyless Identity (/keyless-identity)

All 49 steps → (/inventive-steps)

Identity from accumulated continuity. Post-quantum by construction.

U.S. 19/388,580 (/patents/19-388580)

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

- 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)
- Hardware-Anchor Embodiment of the Continuity-Identity Processor (/articles/keyless-identity/continuity-identity-processor-ic)

APPLICATIONS · GENERAL

- Keyless Workload Identity for Serverless Functions: Authenticating Ephemeral FaaS Without a Persistent Keypair (/articles/keyless-identity/serverless-workload-identity)
- Verifiable Agent Identity Without Credentials: Cryptographic Lineage for Distributed AI Agents (/articles/keyless-identity/trust-slope-entanglement)
- Post-Quantum Identity Migration Without a Public-Key Rebuild (/articles/keyless-identity/post-quantum-migration)
- IoT Device Authentication at Fleet Scale Without Keys or Certificates (/articles/keyless-identity/iot-authentication)

- Keyless Financial Identity Verification Without Credential Databases (/articles/keyless-identity/financial-identity-verification)
- Patient Matching Without a National Identifier: Keyless Identity for Cross-Institutional Patient Continuity (/articles/keyless-identity/healthcare-patient-continuity)
- Supply Chain Authentication Without PKI (/articles/keyless-identity/supply-chain-authentication)
- Keyless Smart Building Access Control: Credential-Free Entry Through Behavioral Continuity (/articles/keyless-identity/smart-building-access)
- Stopping Relay Attacks and Fob-Sharing: Binding Vehicle Access to the Driver, Not the Key (/articles/keyless-identity/vehicle-operator-identity)
- Refugee Identity Without Documents: A Keyless, Database-Free Approach (/articles/keyless-identity/refugee-identity)
- Licensing Keyless Identity at the Silicon Layer: Component-Level IP for Verifiable Device Provenance (/articles/keyless-identity/silicon-vendor-licensing)
- How Do Agents Prove Identity Without a Static Secret or an Issuer? The Market Is Converging on Keyless Continuity (/articles/keyless-identity/agent-identity-convergence)
- Drone Swarm Identity Under Jamming: Keyless Authentication When There Is No Certificate Authority to Reach (/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)
- Authenticating Spaceborne and Interplanetary Links: Keyless Identity for Delay-Tolerant Networks With No Reachable Certificate Authority (/articles/keyless-identity/spaceborne-dtn-authentication)
- Authenticating Federated Learning Nodes Without Keypairs or a Certificate Authority (/articles/keyless-identity/federated-learning-node-authentication)
- **When the Credential Is Stolen and Still Valid (/articles/keyless-identity/keyless-identity-stakes)**

APPLICATIONS · SPECIFIC

- Okta Alternative for Keyless Identity: Federated IdP vs Credential-Free Continuity (/articles/keyless-identity/okta)
- Auth0 Alternative: Keyless Identity Beyond Stored Credentials (/articles/keyless-identity/auth0)
- YubiKey Alternative for Keyless Identity: Beyond the Stored Private Key (/articles/keyless-identity/yubico)
- CLEAR Alternative: Biometric Identity Without a Stored Template Database (/articles/keyless-identity/clear)
- Worldcoin Scans Irises to Prove Humanity. The Proof Depends on a Central Enrollment System. (/articles/keyless-identity/worldcoin)

- Jumio Alternative for Continuity-Based Identity: Keyless Identity Beyond Document Verification (/articles/keyless-identity/jumio)
- Microsoft Entra Alternative: Keyless Identity Beyond Stored Credentials (/articles/keyless-identity/microsoft-entra)
- Ping Identity vs Keyless Identity: A Post-Quantum Alternative to PKI-Bound Federation (/articles/keyless-identity/ping-identity)
- OneLogin Alternative: Keyless Identity Beyond the Stored SSO Credential (/articles/keyless-identity/onelogin)
- Duo Security Made MFA Ubiquitous. The Second Factor Is Still a Credential. (/articles/keyless-identity/duo-security)
- Thales HSM vs Keyless Identity: Protecting Keys or Eliminating Them? (/articles/keyless-identity/thales-hsm)
- Entrust Alternative: Keyless Identity Beyond Certificate-Based Trust (/articles/keyless-identity/entrust)
- DigiCert Alternative for Keyless Identity: Beyond Certificate-Chain Trust (/articles/keyless-identity/digicert)
- Let's Encrypt Alternative: Keyless Identity Beyond the Certificate Model (/articles/keyless-identity/lets-encrypt)
- Qorvo Secure Element Alternative: Continuity Identity Above the Root of Trust (/articles/keyless-identity/qorvo-secure-element)
- NXP EdgeLock Secure Element Alternative: Continuity Above Key Custody (/articles/keyless-identity/nxp-trust-anchor)
- Infineon OPTIGA Alternative: Keyless Continuity Identity Beyond Stored-Key Roots (/articles/keyless-identity/infineon-secure-microcontroller)
- Microchip Trust Platform Alternative: Keyless Identity Above the Secure Element (/articles/keyless-identity/microchip-trust-platform)
- Indicio SSI alternative: keyless identity beyond wallet-held keys (/articles/keyless-identity/indicio-ssi)
- Sovrin Foundation Alternative: Keyless Identity Beneath Self-Sovereign Identity (/articles/keyless-identity/sovrin-foundation)
- W3C DIDs vs keyless identity: who holds the controller's keys? (/articles/keyless-identity/w3c-dids)
- W3C Verifiable Credentials and Keyless Holder Binding (/articles/keyless-identity/w3c-verifiable-credentials)
- Keycard Alternative: Issuer-Free Agent Identity Beyond Token-Based IAM (/articles/keyless-identity/keycard)

- Aembit Alternative: Carried Continuity Beyond External Attestation (/articles/keyless-identity/aembit)
- Astrix Security Alternative: Keyless Identity Beneath the NHI Governance Overlay (/articles/keyless-identity/astrix-security)
- Oasis Security Alternative: Keyless Non-Human Identity Beyond External Lifecycle Anchoring (/articles/keyless-identity/oasis-security)
- Token Security Alternative: NHI Catalog vs. Keyless Cryptographic Continuity (/articles/keyless-identity/token-security)
- Entro Security Alternative: Secret Discovery vs. Keyless Secret Elimination (/articles/keyless-identity/entro-security)
- SPIFFE/SPIRE alternative: workload identity without a certificate authority or persistent keypair (/articles/keyless-identity/spiffe-spire)
- HashiCorp Vault vs a keyless trust slope: where does the identity of the caller come from? (/articles/keyless-identity/hashicorp-vault)

HOW-TO GUIDES

- How to Authenticate Devices on a Jammed or Disconnected Network (/articles/guides/authenticate-devices-on-disconnected-network)
- How to Authenticate Users Without Passwords or Stored Keys (/articles/guides/authenticate-without-passwords-or-keys)
- How to Encrypt Messages Without PKI or a Key Exchange (/articles/guides/encrypt-messages-without-pki)
- How to Move to Post-Quantum Identity Without PKI (/articles/guides/post-quantum-identity-without-pki)

TERMINOLOGY

- dynamic signature mesh (/glossary#dynamic-signature-mesh)
- memory-resolved identity (/glossary#memory-resolved-identity)

Keyless Identity overview → (/keyless-identity)