Nick Clark · Published April 25, 2026 · PDF

Authenticating Federated Learning Nodes Without Keypairs or a Certificate Authority

Federated learning trains a shared model across many nodes that never pool their raw data, but every training round still asks each node to prove it is the same trusted participant, and the usual answer is a persistent keypair backed by a certificate authority that becomes a single point of compromise and a correlation handle. This article shows how that node-authentication problem can be addressed using the Keyless Identity, disclosed in United States Patent Application 19/388,580. Identity is expressed as a locally reconstructed trust slope rather than a standing credential, so nodes authenticate one another and the coordinator by memory-resolved behavioral continuity instead of by a registry of long-lived keys.

What This Application Specifies

United States Patent Application 19/388,580 discloses a memory-native identity and authentication architecture that operates without persistent public-private keypairs and without external verification authorities. Instead of presenting a static credential, a device or agent expresses identity as a trust slope: the cumulatively validated sequence of Dynamic Device Hashes (DDH) or Dynamic Agent Hashes (DAH) formed by successive, verifiable identity mutations. Each step is computed from the immediately prior step combined with a source of non-exported unpredictability and a volatile, non-repeating salt, under a published update rule with a domain-separating tag.

The unpredictability contribution comes from one of three interchangeable sources described in the disclosure: a static hardware anchor combined with a per-epoch volatile salt, a locally observed state vector processed by a strong extractor into a bounded token, or a hybrid that concatenates both in the same step. A receiver stores any previously trusted step and validates a presented successor against policy-bounded continuity criteria, reconstructing the expected successor locally. Because each step binds to the prior step and to unpredictability that never leaves the originating node, a party lacking that local state cannot feasibly synthesize valid successors.

The disclosure also specifies two-stage message authentication in which the current dynamic hash is placed in the transport header for fast stateless screening and the same value is embedded inside a payload encrypted under a symmetric key derived transiently from the recipient's current identity; append-only mutation lineage with periodic anchors for tamper-evident provenance; delayed and sparse validation using bounded proof windows for intermittently connected participants; entropy-anchor rotation with forward links; and quorum-based recovery after memory loss using attestations from previously trusted peers.

Why It Matters

Federated learning exists precisely because the raw data cannot be centralized, whether for privacy, regulatory, or bandwidth reasons. Cross-silo deployments span hospitals, banks, and manufacturers; cross-device deployments span phones, vehicles, and edge sensors. In both cases a coordinator repeatedly invites nodes to download the current model, train locally, and return an update. The security question that runs underneath every round is deceptively simple: is this the same node we trusted last round, and is this update actually from it?

The prevailing answer is a public key infrastructure. Each node holds a long-lived keypair, a certificate authority vouches for it, and updates are signed. That arrangement inherits every weakness the disclosure catalogs for conventional systems: key

compromise gives an attacker a durable impersonation capability, the certificate becomes a stable identifier that lets a coordinator or an observer correlate a node's activity across rounds and campaigns, certificate revocation must propagate reliably or a compromised node keeps participating, and the whole structure leans on a centralized trust anchor that decentralized training was supposed to avoid. For memory-constrained edge participants, maintaining and protecting persistent private key material is itself a burden, and the disclosure notes that in ephemeral or stateless substrates the requirement to hold static credentials is impractical.

Keyless Identity removes the standing secret from the authentication path. There is no key to steal that yields lasting impersonation, no certificate to correlate across rounds, and no authority whose compromise unravels the federation. That reframing is what makes it a direct fit for distributed training, and the disclosure names federated learning and distributed AI ecosystems explicitly among its target environments.

How It Composes With the Domain

Map the training topology onto the disclosed roles. Each participating node is a host maintaining its own DDH; a training job carried between a node and the coordinator can be treated as a memory-bearing agent maintaining a DAH. Enrollment establishes a slope root for each node from that node's local unpredictability source, so a hospital server with a hardware security module can anchor on its hardware identifier plus volatile salts, while a lightweight edge device can anchor on a stability-tuned local state vector processed by the extractor. No node registers a public key, and the coordinator maintains no certificate store.

Each training round advances the slope. When a node submits its model update, it presents the current dynamic hash in the transport header, and the coordinator performs the fast continuity check: it reconstructs the expected successor from the last trusted state it holds for that node and confirms the presented value is an on-slope successor under policy-bounded continuity parameters. The update payload is

encrypted under a symmetric key derived from the recipient's current identity, and the sender's dynamic hash is embedded inside the encrypted payload. The coordinator screens the header before decryption, derives its decryption key from its own current identity, and then validates the embedded sender hash against the sender's reconstructed slope. An update is accepted only when both the header and the embedded value validate, which binds routing-level and content-level integrity together and rejects a substituted update after decryption.

Because each step carries a mutation class recording the semantic reason for the transition, a round-to-round update, a role change, or a delegation can be labeled and later audited. The disclosure's predictive verification composes naturally here: a cadence estimator and a role-transition model forecast the expected next successor and an acceptance envelope, so a node that suddenly deviates from its established behavioral trajectory, in timing or in token-space neighborhood, is surfaced as drift before it fully breaks continuity. For a training operator, that is an early signal that a participant is behaving unlike itself.

Straggler and disconnection tolerance is built in rather than bolted on. Cross-device federated learning is notorious for nodes that drop out mid-round and return later. The disclosed delayed-validation path lets a returning node present a bounded set of per-step mutation proofs representing its slope evolution since a previously trusted anchor; the coordinator replays those steps locally to re-establish continuity without any global synchronization or external registry. Sparse checkpointing bounds how much a memory-constrained device must retain. If a device loses its lineage entirely, for example after a reset, the quorum-based recovery path lets it rejoin by aggregating signed attestations from previously trusted peers into a recovery token that is stitched into its lineage, restoring continuity without reissuing any credential.

Agent-to-substrate entanglement adds provenance that federated learning specifically wants. When a training agent mutates on a given node, the host emits a signed entanglement trace binding that mutation to the node's device identity at execution

time, and the agent folds the trace into a cumulative commitment. A verifier accepts the successor only if the trace opens to the host's DDH under policy. The result is a tamper-evident record that ties each model update to the specific node that produced it, which supports attribution and forensic reconstruction across the federation without a central ledger.

What This Enables

A federated training deployment can run without a certificate authority in the trust path, removing the centralized anchor and the revocation machinery that decentralized learning otherwise reimports. Nodes authenticate one another and the coordinator by verifiable behavioral continuity, so trust graphs can form organically across administrative boundaries such as separate institutions in a cross-silo consortium.

The absence of a persistent per-node identifier constrains linkability. The disclosure describes rotating the transport-header hash on a policy-defined cadence with forward links, so an observer or a coordinator cannot use a stable certificate to correlate a node's participation across rounds or across training campaigns while continuity remains verifiable under bounded proofs.

Update authenticity gains an entanglement-backed provenance trail. Because each accepted update carries a mutation lineage anchored to the producing node's device identity, an operator investigating an anomalous global model can reconstruct which node contributed which update and confirm that no entry was omitted or reordered, using only locally held anchors and bounded disclosures. This does not by itself judge whether an update is statistically poisoned, but it does make the origin and integrity of each update verifiable, which is the foundation any poisoning defense builds on.

The model also suits the heterogeneity of real federations. Powerful silo servers, commodity phones, and ultra-low-power sensors can each pick the unpredictability source that fits their platform while remaining interoperable in the same federation,

because validation logic is uniform across the hardware-anchor, local-state, and hybrid embodiments. And because identity rests on local unpredictability and hash-based commitments rather than on hardness assumptions targeted by Shor-type algorithms, the deployment is post-quantum aligned by construction, which matters for training relationships expected to persist for years.

Boundary Conditions

Keyless Identity authenticates participants and secures the provenance and integrity of their updates. It does not evaluate the statistical content of a model update, so it is not on its own a defense against a genuinely enrolled but malicious node that submits carefully crafted poisoned gradients; that node presents a valid on-slope successor. What the disclosure provides is verifiable attribution and tamper evidence for each update, which a separate robust-aggregation or anomaly-detection layer can build upon.

Continuity depends on locally retained state and unpredictability. A node that loses its lineage cannot simply reissue itself; it must go through the quorum-based recovery path, which requires enough previously trusted peers to be reachable and to attest under the governing quorum policy. In small federations or during mass reconnection events, operators must provision that peer set and policy deliberately.

The continuity policy is a tuning surface, not a default. The acceptance radius, cadence bounds, replay horizon, and quorum thresholds must be calibrated to the deployment. Envelopes set too tight cause spurious rejections when a node's local conditions shift benignly; set too loose, they weaken drift detection. The disclosure provides stability-tuned projections and error-tolerant sketches to widen the safe operating band, but the parameters remain a deployment responsibility.

Finally, interoperability with existing PKI-based training infrastructure runs through the disclosed legacy-bridge adapter, which is deliberately isolated: fallback identifiers and their signatures are never hashed into slope evolution, and any attempt to mix them fails closed. That isolation is a feature for security, but it means a phased rollout coexisting with a legacy coordinator carries two authentication paths during migration.

Disclosure Scope

The identity and authentication mechanisms described here, including the trust slope, dynamic device and agent hashes, the two-stage message authentication, append-only mutation lineage with periodic anchors, delayed and sparse validation, entropy-anchor rotation, quorum-based recovery, and agent-to-substrate entanglement, are disclosed in United States Patent Application 19/388,580 and are recited here as that application describes them. The federated learning and distributed AI training framing in this article, including the mapping of coordinators and participating nodes onto the disclosed roles, cross-silo and cross-device topologies, straggler handling, and model-update provenance, is external application context offered as one enabling implementation and is not itself part of the disclosure. Characterizations of conventional public key infrastructure, certificate authorities, and their operational weaknesses, and any references to regulatory or privacy motivations for federated learning, are provided as domain background and should be independently verified against the reader's own environment; they are not representations about the disclosed subject matter. Nothing here should be read to add performance, benchmark, or security-quantification claims beyond what the application itself states.

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)**

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)

Keyless Identity overview → (/keyless-identity)