Nick Clark · Published April 25, 2026 · PDF

Authenticating Spaceborne and Interplanetary Links: Keyless Identity for Delay-Tolerant Networks With No Reachable Certificate Authority

A spacecraft on a deep-space link cannot reach a certificate authority, an OCSP responder, or a token issuer within any timeframe that authentication assumes, because the round trip is minutes to hours and the link is scheduled, one-way for long stretches, and frequently broken. Yet each node in a delay-tolerant or interplanetary network still has to prove that an arriving bundle came from the peer it claims and not from a replay or a spoof. This application is built on Keyless Identity, disclosed in United States Patent Application 19/388,580, which makes identity a locally reconstructable trust slope validated from bounded proofs rather than a credential checked against an authority in real time, so authentication survives when the link is delayed, one-way, or disconnected for long intervals.

What This Application Specifies

Delay-tolerant networking (DTN) is the architecture built for links where the assumptions of ordinary networking do not hold: round-trip times measured in minutes or hours, contacts that open and close on an orbital or planetary schedule, and long stretches where a node holds data and forwards it later because there is no continuous

end-to-end path. This is the regime of deep-space relays, planetary orbiters and landers, and the store-and-forward bundle transfers that move science and command traffic across an interplanetary network. The standardized bundle protocol used in this regime moves self-contained bundles hop by hop, and each receiving node must decide whether an arriving bundle is authentic before it acts on it or forwards it onward.

This application specifies how the Keyless Identity mechanism disclosed in United States Patent Application 19/388,580 supplies that authentication decision without requiring any node to reach an external authority at the moment of validation. In the disclosed model, a device or agent expresses its identity as a trust slope: an append-only sequence of dynamic hashes (a Dynamic Device Hash, DDH, or Dynamic Agent Hash, DAH), where each successor is computed from the immediately prior value and a source of locally retained unpredictability under a published update rule. A receiver validates a presented identity by checking that it is a valid successor of a state it has previously accepted, using only locally held materials and policy-bounded continuity checks. The specification names spaceborne links directly as a target environment, describing authentication under delayed verification and bounded proof windows for high-latency, disrupted, or disconnected networks including delay-tolerant, mesh, opportunistic, and spaceborne links.

Why It Matters

Every widely deployed authentication model that a ground network relies on assumes reachability, and a deep-space link is defined by its absence. Public-key infrastructure validates a certificate by checking it against an authority and, in practice, checking revocation status; on a link where the round trip is measured in minutes to hours and contacts are scheduled, the responder cannot be consulted inside any window that a live protocol allows. Session-oriented handshakes fail for a related reason: a challenge-response or asymmetric key exchange needs a timely round trip, and on a one-way or long-delayed link there is no timely round trip to complete. Pre-shared symmetric keys

are reachable but brittle across a fleet, because a key distributed to every node so members can authenticate becomes a single point of catastrophic failure the moment any one node is compromised or its key is exposed over a long mission lifetime.

The consequence on a real mission is that authentication either degrades into trusting unvalidated traffic or refuses to operate when the link is exactly what it was designed to be. The disclosed mechanism matters here because it moves the proof of identity into something the node already carries and can reconstruct locally. There is no certificate to check against an unreachable registry, no live handshake to complete across a light-hour of delay, and no fleet-wide shared secret whose exposure unravels the constellation, because each node's trust slope is its own and advances only through the identity mutations it actually performed.

How It Composes With the Domain

A DTN bundle is self-contained and travels through custody transfers, held and forwarded by intermediate nodes until a contact opens. The disclosed mechanism maps onto this shape directly. A sending node advances its trust slope and constructs a message with the current dynamic hash placed in the transport header and the same value embedded inside the protected payload; the symmetric key that protects the payload is derived transiently from the recipient's current dynamic identity, so the message itself carries no key. On receipt, the node performs the disclosed two-stage validation: a fast, stateless continuity screen of the header hash against its last trusted successor lets it reject obvious spoofs and malformed traffic before spending any effort on decryption, and after decryption it validates the embedded sender hash against the reconstructed sender slope. Both stages use only locally retained state and policy-bounded continuity parameters.

The property that makes this work across a delayed or broken link is the disclosed delayed-validation and sparse-recovery path. A node that has been out of contact will not hold the sender's most recent trusted anchor. Rather than fail, the sender includes a

bounded set of mutation proofs, per-step materials sufficient for the verifier to deterministically recompute the intervening successors from its last trusted anchor forward to the presented identity, optionally referencing a periodic anchor or checkpoint to bound the replay. The verifier replays those steps locally, and if the recomputed terminal value matches the presentation and opens to the trusted anchor, the presentation is accepted. Where the verifier's stored state predates the referenced anchor or the supplied proof is insufficient, it can defer final acceptance and request a bounded checkpoint on a later contact, without ever contacting an external registry. Because the identity process is append-only with periodic anchors, nodes retain only sparse selected identities and checkpoints and reconstruct the rest on demand, which suits the storage limits of a spacecraft avionics stack.

Several disclosed provisions compose naturally with the mission profile. Replay resistance is enforced by binding acceptance to monotonic progression along the slope and rejecting reuse of previously accepted successors within a policy horizon, which is exactly the protection a store-and-forward network needs when the same bundle may be seen more than once. Entropy-anchor rotation with recorded forward links lets a long-lived spacecraft refresh its identity epoch over a multi-year mission without breaking auditability, since a verifier bridges old and new epochs through the forward link under policy. Where a node must interoperate with legacy signature-based ground equipment, the disclosed fallback path confines a transient keypair to a segregated adapter whose materials never feed back into the trust slope, so interoperability does not dilute the no-persistent-keypair property among the space nodes themselves.

What This Enables

The composition enables authentication native to the link rather than fighting it. A relay node can accept a bundle on a scheduled contact, hold it, and forward it later, and the receiving custodian can validate its origin from carried proofs whenever it next processes the bundle, with no requirement that any authority be reachable at either moment. An orbiter that has been over the far side of a body, or a lander powered down

through a night, can re-establish continuity from bounded proofs and, if it has lost state entirely, through the disclosed quorum recovery, in which previously trusted peers issue attestations that aggregate into a recovery token under a quorum policy, so a node rejoins the trust graph through a threshold of peer validations rather than a call home. Because security here reduces to the unpredictability of per-step inputs and the preimage resistance of the hashes and extractors rather than to hardness assumptions vulnerable to Shor-type attacks, the model is post-quantum aligned by construction, which matters for missions whose design lifetime outruns the migration timelines of certificate-based systems. And because no node holds a fleet-wide secret or a long-lived private key, the loss of one spacecraft is a contained, attributable event rather than a disclosure that compromises the constellation.

Boundary Conditions

This application is an enabling implementation, and its honest limits should be stated. The disclosed mechanism authenticates identity continuity and message provenance; it is not an orbital-mechanics or contact-scheduling system, and it presumes the underlying bundle transport delivers bundles eventually, however delayed. Delayed validation requires that a verifier hold, or be able to obtain on a later contact, a checkpoint or anchor from which to replay; a verifier whose trusted state is older than the available proof window must wait for a bounded checkpoint before it can accept, which trades immediate acceptance for the ability to operate disconnected. The strength of the guarantee depends on the min-entropy of the per-step unpredictability contribution, so a constrained spacecraft endpoint must be provisioned with an adequate unpredictability source, whether a hardware anchor with per-epoch volatile salt, a local-state derivation, or a hybrid of both. Continuity policy must be tuned to the mission: acceptance envelopes set too tightly will reject legitimate drift after long dormancy, while envelopes set too loosely weaken spoof rejection. None of the

numbers, latencies, or mission parameters that a specific deployment would need are asserted here; they are engineering choices for the integrator, and this article does not claim any measured performance for the mechanism on a space link.

Disclosure Scope

The keyless identity mechanism described here, including the append-only trust slope of dynamic hashes advanced by locally retained unpredictability, the transiently derived symmetric keys and two-stage header-and-payload validation, the delayed validation and sparse recovery using bounded proof windows and periodic anchors, the replay resistance through monotonic slope progression, the entropy-anchor rotation with forward links, the predictive drift triage, the quorum-based recovery after state loss, and the strictly isolated legacy fallback path, is disclosed in United States Patent Application 19/388,580. This article applies those disclosed mechanisms to the delay-tolerant and interplanetary networking condition, in which links are high-latency, scheduled, frequently one-way, and disconnected for long intervals. References to delay-tolerant networking, the bundle protocol, and space communication architecture are to public standards and domain facts and are used for context only; they are external framing, not part of the disclosed technology. This article is an application of the disclosed technology and is not itself a patent claim.

Keyless Identity (/keyless-identity) All 40 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)

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)