Ping Identity Built Enterprise Federation. The Federation Depends on Shared Secrets.

by Nick Clark | Published March 28, 2026 | PDF

Ping Identity provides enterprise federation, single sign-on, and API security through industry-standard protocols including SAML, OAuth 2.0, and OpenID Connect. The federation model allows identities to be asserted across organizational boundaries. But every federation relationship depends on shared secrets: signing certificates, client secrets, and token encryption keys that both parties must maintain. A compromised federation certificate breaks the trust relationship across every relying party. The gap is between federated identity management and an identity primitive that does not depend on shared key material.

Ping Identity's federation depth, adaptive authentication, and API security capabilities serve real enterprise needs. The gap described here is about the federation protocol's dependency on shared secrets, not about Ping's implementation quality.

Federation requires shared key material

SAML federation requires signing certificates exchanged between the identity provider and each service provider. OAuth 2.0 requires client secrets or certificate-based client authentication. OpenID Connect adds ID tokens signed with keys that relying parties must be able to verify. Every federation relationship is built on shared or published key material.

When these keys are compromised, rotated, or expired, the federation relationship breaks until new key material is exchanged. The operational burden of certificate management across hundreds of federation relationships is substantial. The key material is the foundation that federation trust stands on.

Token-based identity is credential-based identity

Federation produces tokens: SAML assertions, OAuth access tokens, and OIDC ID tokens. These tokens are time-limited credentials. They must be stored during their lifetime, transmitted securely, and validated at each relying party. A stolen token provides the bearer with the identity it represents until the token expires.

Shorter token lifetimes reduce the window of vulnerability but increase the frequency of authentication events. The fundamental model remains: identity is proven by presenting a credential artifact.

What keyless identity addresses

Keyless identity would enable federation without shared secrets. Each party's identity would derive from its accumulated behavioral continuity, validated through trust slope functions. A federation relationship would not depend on exchanged certificates or shared keys. It would depend on the continuous behavioral validation of each participating entity.

A compromised certificate would not break the federation because the federation does not depend on certificates. Each entity's identity is its own continuity, independently verifiable without shared material.

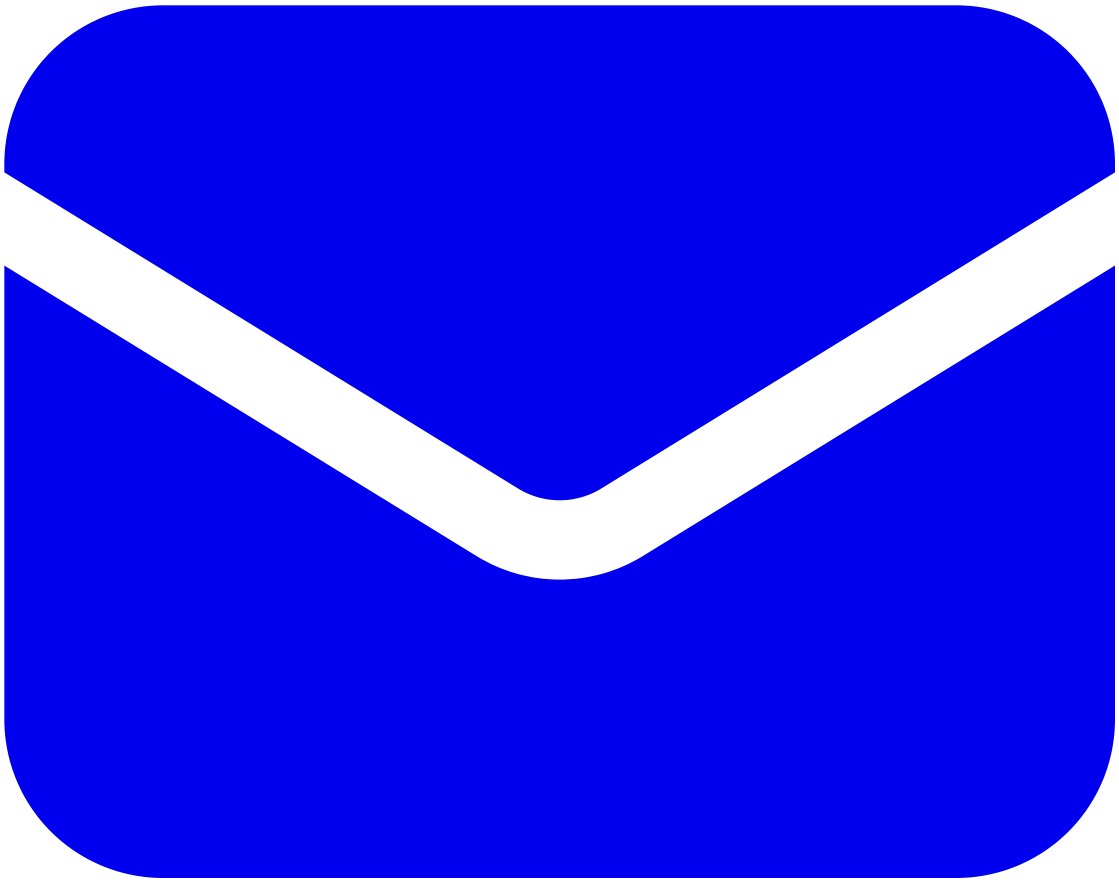
Keyless Identity All 21 steps →

Identity from accumulated continuity. Post-quantum by construction.

Patent
US 19/388,580 · published
Primary Technical Disclosure
○ Stateless Device Pseudonymity and Secure Messaging in Cognition-Native Systems
Secondary Technical
○ Continuity-Based Biological Identity Using Trust-Slope Validation○ Trust Slope as Identity Primitive: Cumulative Hash Chains Replace Static Credentials○ Dual-Source Identity Derivation: Hardware Anchors and Local State Vectors Combined Per Epoch○ Stateless Symmetric Encryption: Session Keys Derived From Current Identity State○ Two-Stage Message Authentication: Transport Continuity Screening Before Semantic Validation○ Agent-Substrate Slope Entanglement: Binding Every Mutation Step to Its Execution Host○ Append-Only Mutation Lineage Log: Forward-Secure Identity Transition Chains○ Cumulative Slope Validation Across Substrates: Multi-Node Provenance Verification○ Quorum-Based Identity Recovery: Peer Attestation After Memory Loss○ Entropy Anchor Rotation: Proactive Identity Reseeding With Forward Links○ Biometric-Assisted Reseeding: Privacy-Preserving Fuzzy Extractors for Anchor Rotation○ Delayed Slope Validation: Bounded Proof Windows for Disconnected Environments○ Sparse Trust Slope Recovery: Compact Checkpoints for Resource-Constrained Devices○ Predictive Identity Validation: Drift Detection Before Full Discontinuity○ Legacy PKI Fallback: Session-Scoped Adapters With Strict Isolation Boundaries○ Post-Quantum Alignment: Hash-Based Security Without Vulnerable Hardness Assumptions
Applications (General)
○ Trust Slope Entanglement: Cryptographic Lineage for Semantic Agents○ Post-Quantum Enterprise Identity Migration○ Billions of IoT Devices Need Authentication Without Keys○ Financial Identity Without Credential Databases○ Patient Identity Through Behavioral Continuity○ Supply Chain Authentication Without PKI○ Smart Building Access Through Continuity○ Vehicle Operator Identity Binding○ Displaced Person Identity Without Documents
Applications (Specific)
○ Okta Centralized Enterprise Identity. The Keys That Prove It Are Still Stored Somewhere.○ Auth0 Made Developer Identity Easy. The Credential Model Underneath Did Not Change.○ YubiKey Made Hardware Authentication Practical. The Key Is Still the Vulnerability.○ CLEAR Made Airport Identity Fast. It Built a Biometric Database to Do It.○ Worldcoin Scans Irises to Prove Humanity. The Proof Depends on a Central Enrollment System.○ Jumio Automated ID Verification. The Verification Still Depends on Documents.○ Microsoft Entra Unified Cloud Identity. Identity Still Depends on Stored Credentials.● Ping Identity Built Enterprise Federation. The Federation Depends on Shared Secrets.○ OneLogin Simplified Enterprise SSO. The SSO Token Is Still a Credential.○ Duo Security Made MFA Ubiquitous. The Second Factor Is Still a Credential.○ Thales HSMs Protect Key Material. The Keys Still Exist.○ Entrust Issues Digital Certificates. The Certificate Is a Stored Credential.○ DigiCert Secures the Web With TLS Certificates. The Certificate Model Has Structural Limits.○ Let's Encrypt Made TLS Free. The Certificate Model Is Still the Same.
Keyless Identity overview →
AQ
deterministic
autonomy

Legal

Last updated: 2026-03-03



-
- nick@qu3ry.net
- 72 28 14 36 01

Invented by Nick Clark | Founding Investors: Devin Wilkie