OneLogin Simplified Enterprise SSO. The SSO Token Is Still a Credential.

by Nick Clark | Published March 28, 2026 | PDF

OneLogin simplified enterprise single sign-on by providing a unified portal for accessing applications with directory integration, risk-based adaptive authentication, and SmartFactor authentication. Users authenticate once and receive access to all configured applications. But the SSO model produces session tokens and SAML assertions that are stored credentials with finite lifetimes. A stolen session token provides full access until it expires. The structural gap is between streamlined authentication flows and an identity model where no tokens need to be stored because identity derives from continuous behavioral validation.

OneLogin's approach to simplifying enterprise SSO and its SmartFactor authentication reduced friction for enterprise users. The gap described here is about the SSO model's dependency on session credentials, not about OneLogin's product design.

SSO concentrates credential risk

Single sign-on is valuable because users authenticate once. But the corollary is that the single authentication event produces a session credential that unlocks everything. The SSO session token is the most valuable credential in the enterprise because it provides access to all connected applications.

Session hijacking, token theft, and cookie stealing attacks target SSO sessions specifically because a single compromised session provides broad access. Protecting this concentrated credential is more critical than protecting any individual application credential.

Adaptive authentication adds layers, not elimination

OneLogin's risk-based authentication evaluates context signals before granting access: device fingerprint, IP reputation, login patterns. When risk is elevated, additional authentication factors are required. These are layers of protection around the credential exchange, not elimination of the credential.

After adaptive authentication succeeds, the result is still a session token that must be stored and can be stolen. The authentication was more thorough. The credential it produced is the same structural artifact.

What keyless identity addresses

Keyless identity replaces the session token model with continuous behavioral validation. Instead of authenticating once and receiving a credential, identity is continuously derived from the device's behavioral continuity through trust slope validation. There is no session token to steal because access is continuously validated, not granted and cached.

OneLogin's application integration and directory synchronization would continue to provide the management layer. The identity primitive would shift from token-based sessions to continuous behavioral validation through keyless identity.

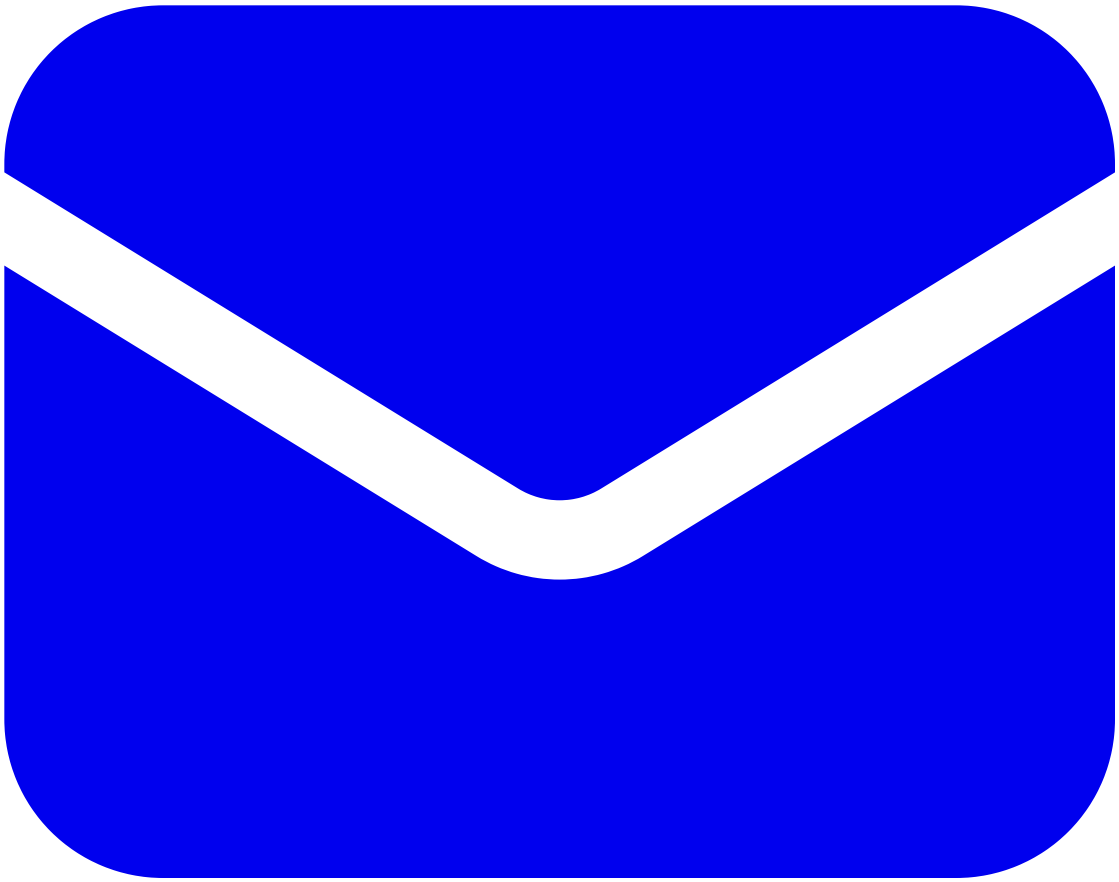
Keyless Identity All 21 steps →

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