Entrust Issues Digital Certificates. The Certificate Is a Stored Credential.

by Nick Clark | Published March 28, 2026 | PDF

Entrust provides digital certificates, PKI infrastructure, and identity verification solutions used by enterprises, financial institutions, and governments worldwide. The certificate authority infrastructure is mature and trusted. But every digital certificate is a stored credential with a fixed lifetime. It must be issued by a trusted authority, stored securely by the holder, rotated before expiration, and revoked if compromised. Certificate lifecycle management is a permanent operational burden. The structural gap is between well-managed certificates and an identity model that does not require issuing, storing, or revoking credential material.

Entrust's certificate authority infrastructure and identity verification capabilities serve critical functions in global commerce and government identity. The gap described here is about the certificate model, not about Entrust's operational reliability.

Certificate lifecycle is permanent overhead

Every certificate Entrust issues begins a lifecycle: issuance, deployment, monitoring, renewal, and eventual expiration or revocation. Across an enterprise with thousands of certificates for TLS, code signing, email, and device identity, the lifecycle management overhead is substantial. Expired certificates cause outages. Compromised certificates require emergency revocation.

Automated certificate management tools reduce the operational burden but do not eliminate the underlying model: identity depends on a time-limited credential that must be continuously maintained.

Revocation is a structural weakness

When a certificate is compromised, revocation must propagate to all relying parties. CRL distribution and OCSP responses have latency. During the propagation window, a revoked certificate may still be trusted by parties that have not yet received the revocation update. The revocation model is eventually consistent at best.

Certificate pinning, stapling, and short-lived certificates mitigate revocation latency but add complexity. Each mitigation addresses a symptom of the underlying structural dependency on stored, time-limited credentials.

What keyless identity addresses

Keyless identity eliminates the certificate lifecycle entirely. Identity derives from accumulated behavioral continuity, not from issued credentials. There is no issuance, no expiration, no revocation, and no renewal. The identity continuously validates through trust slope functions. Compromise of a device does not require revocation because the compromised device's behavioral continuity diverges from its accumulated history, and the trust slope validation detects the divergence.

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

-
- Inventive Steps
- Licensing
- Patents
- Articles
- Legal
- Opportunities
- Sitemap

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

Invented by Nick Clark | Founding Investors: Devin Wilkie