Nick Clark · Published June 22, 2026 · PDF

Forced Off the Keys: Why the Post-Quantum Migration Points Past PKI to Keyless

Governments have set hard deadlines for abandoning the public-key cryptography the internet runs on, and the standards replacing it are increasingly hash-based, betting on preimage resistance. The migration is forcing the world onto the exact foundation keyless identity is built on, while everyone else stops one step short, still issuing keys.

A Deadline With Hard Dates

Governments have stopped treating the migration away from classical public-key cryptography as a long-term research concern and started setting deadlines. The public-key algorithms the internet runs on, RSA and the elliptic-curve schemes, are breakable in principle by a sufficiently large quantum computer, and the response is now a scheduled, mandated transition rather than a debate. The United States has finalized post-quantum standards and directed federal migration on a defined timeline; allied governments have published coordinated roadmaps with explicit milestone years; and procurement and compliance regimes are beginning to require post-quantum readiness as a condition of doing business. The migration is no longer optional and no longer distant. What it points at, on close reading, is not merely a swap of one signature algorithm for another.

The Pattern in the Replacements

Look at what the standards bodies actually chose. Among the finalized post-quantum signature standards is a hash-based scheme whose security rests on the difficulty of inverting a hash function, the preimage problem, rather than on the algebraic structure a quantum computer exploits. National security guidance for signing firmware and software has specifically named stateful hash-based signature schemes for that purpose. National technical authorities in Europe have expressed a preference for hash-based approaches where they fit, on the grounds that their security assumptions are the most conservative and best understood. The through-line is clear: when the requirement is long-term, conservative, future-proof integrity, the field is moving toward security founded on hash-preimage hardness.

There is a second pattern alongside the first. The same regulatory direction is pushing toward credentials that are short-lived and freshly produced rather than long-lived and stored, and toward unlinkability requirements that discourage a single persistent key from following a subject across contexts. The field is simultaneously moving to preimage-based security and to ephemeral, non-persistent credentials. Both are steps in the same direction, and both stop one step short of the obvious conclusion.

The Step Not Taken

For all of that movement, the migration has not gone keyless. The hash-based signature schemes are post-quantum, but they still hold a private key whose disclosure forges signatures. The ephemeral-credential systems reseed from key material; the ratchets that rotate session keys still begin from a keypair; the wallets that hold post-quantum credentials are still bound to a device keypair. The field has adopted preimage security and adopted short-lived credentials, but it has kept the stored secret. It has migrated the algorithm and preserved the architecture.

The destination the migration implies but has not reached is identity that is secured by exactly the preimage hardness the standards bodies are betting on, and that holds no stored key at all. Keyless identity is an evolving, device-entangled hash chain: its security rests on the same one-way-function assumption as the hash-based signature standards, its credential is computed from continuity rather than stored, it is naturally ephemeral because each state supersedes the last, and it is naturally unlinkable because there is no persistent key to correlate. Crucially, there is nothing to harvest. The harvest-now-decrypt-later threat, in which an adversary records today's signed material to break later when quantum computers arrive, has no purchase on an identity that stores no secret to be broken. The migration is forcing the world onto preimage-based security and ephemeral credentials, which is to say onto the exact foundation keyless identity already stands on, while the rest of the field stops at re-issuing keys.

Relation to the Migration Itself

This article is the forcing-function argument: why the post-quantum transition, taken to its logical end, points past key-based public-key infrastructure to keyless identity. The companion piece on post-quantum migration (/articles/keyless-identity/post-quantum-migration) addresses the practical application, how a keyless approach is adopted within an organization's migration program. Read together, one explains why the deadline makes the keyless direction inevitable and the other explains how to move in it.

Disclosure Scope

The keyless identity mechanism, secured by hash-preimage hardness, device-entangled, holding no stored private key, and naturally ephemeral and unlinkable because identity is a computed property of an evolving chain rather than a persistent secret, is disclosed in the identity filing (U.S. Application No. 19/388,580, published as US 2026/0126730 A1). This article frames that disclosed mechanism against the publicly announced post-quantum migration: the finalized hash-based signature standards, the national

guidance favoring hash-based schemes for firmware and long-term integrity, the coordinated migration roadmaps, and the regulatory pressure toward short-lived and unlinkable credentials. It argues that the migration converges on a preimage-based, non-stored foundation that keyless identity already occupies. References to standards and government roadmaps are to their public materials and are used for context only.

Keyless Identity (/keyless-identity)

All 36 steps → (/inventive-steps)

Identity from accumulated continuity. Post-quantum by construction.

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

- Continuity-Based Biological Identity Using Trust-Slope Validation (/articles/continuity-based-biological-identity-using-trust-slope-validation)
- 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)
- Continuity-Identity Processor IC: Silicon-Block Embodiment (/articles/keyless-identity/continuity-identity-processor-ic)
- Biological-Device Binding Through Continuity (/articles/keyless-identity/biological-device-binding)
- Multi-Modal Biometric Continuity Coupling (/articles/keyless-identity/multi-modal-continuity-coupling)

APPLICATIONS · GENERAL

- Trust Slope Entanglement: Cryptographic Lineage for Semantic Agents (/articles/keyless-identity/trust-slope-entanglement)
- Post-Quantum Enterprise Identity Migration (/articles/keyless-identity/post-quantum-migration)
- Billions of IoT Devices Need Authentication Without Keys (/articles/keyless-identity/iot-authentication)
- Financial Identity Without Credential Databases (/articles/keyless-identity/financial-identity-verification)
- Patient Identity Through Behavioral Continuity (/articles/keyless-identity/healthcare-patient-continuity)
- Supply Chain Authentication Without PKI (/articles/keyless-identity/supply-chain-authentication)
- Smart Building Access Through Continuity (/articles/keyless-identity/smart-building-access)
- Vehicle Operator Identity Binding (/articles/keyless-identity/vehicle-operator-identity)
- Displaced Person Identity Without Documents (/articles/keyless-identity/refugee-identity)

- Component-Level Identity Licensing at the Silicon Layer (/articles/keyless-identity/silicon-vendor-licensing)
- The Agent Identity Wave: Where the Whole Market Is Heading (/articles/keyless-identity/agent-identity-convergence)
- When the Link Dies, the Identity Has to Live Onboard (/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)**

APPLICATIONS · SPECIFIC

- Okta Centralized Enterprise Identity. The Keys That Prove It Are Still Stored Somewhere. (/articles/keyless-identity/okta)
- Auth0 Made Developer Identity Easy. The Credential Model Underneath Did Not Change. (/articles/keyless-identity/auth0)
- YubiKey Made Hardware Authentication Practical. The Key Is Still the Vulnerability. (/articles/keyless-identity/yubico)
- CLEAR Made Airport Identity Fast. It Built a Biometric Database to Do It. (/articles/keyless-identity/clear)
- Worldcoin Scans Irises to Prove Humanity. The Proof Depends on a Central Enrollment System. (/articles/keyless-identity/worldcoin)
- Jumio Automated ID Verification. The Verification Still Depends on Documents. (/articles/keyless-identity/jumio)
- Microsoft Entra Unified Cloud Identity. Identity Still Depends on Stored Credentials. (/articles/keyless-identity/microsoft-entra)
- Ping Identity Built Enterprise Federation. The Federation Depends on Shared Secrets. (/articles/keyless-identity/ping-identity)
- OneLogin Simplified Enterprise SSO. The SSO Token Is Still a Credential. (/articles/keyless-identity/onelogin)
- Duo Security Made MFA Ubiquitous. The Second Factor Is Still a Credential. (/articles/keyless-identity/duo-security)
- Thales HSMs Protect Key Material. The Keys Still Exist. (/articles/keyless-identity/thales-hsm)
- Entrust Issues Digital Certificates. The Certificate Is a Stored Credential. (/articles/keyless-identity/entrust)
- DigiCert Secures the Web With TLS Certificates. The Certificate Model Has Structural Limits. (/articles/keyless-identity/digicert)
- Let's Encrypt Made TLS Free. The Certificate Model Is Still the Same. (/articles/keyless-identity/lets-encrypt)

- Qorvo Secure Elements Authenticate, but Don't Track Continuity (/articles/keyless-identity/qorvo-secure-element)
- NXP Trust Anchor Stores Keys, Not Trust Slope (/articles/keyless-identity/nxp-trust-anchor)
- Infineon Secure Microcontrollers Need Continuity Logic On-Die (/articles/keyless-identity/infineon-secure-microcontroller)
- Microchip Trust Platform Fits Hardware, Misses Behavioral Continuity (/articles/keyless-identity/microchip-trust-platform)
- Indicio SSI Network and Anonyome Labs (/articles/keyless-identity/indicio-ssi)
- Sovrin Foundation Self-Sovereign Identity (/articles/keyless-identity/sovrin-foundation)
- W3C Decentralized Identifiers (DIDs) (/articles/keyless-identity/w3c-dids)
- W3C Verifiable Credentials (/articles/keyless-identity/w3c-verifiable-credentials)
- Keycard: Token-Issuer IAM Reaches Toward Identity Continuity (/articles/keyless-identity/keycard)
- Aembit: External Attestation Is Half the Answer (/articles/keyless-identity/aembit)
- Astrix Security: Discovery and Governance Without a Substrate (/articles/keyless-identity/astrix-security)
- Oasis Security: Non-Human Identity Governance, Externally Anchored (/articles/keyless-identity/oasis-security)
- Token Security: NHI Catalog Without Cryptographic Continuity (/articles/keyless-identity/token-security)
- Entro Security: Secret Discovery vs. Secret Elimination (/articles/keyless-identity/entro-security)

Keyless Identity overview → (/keyless-identity)