Duo Security Made MFA Ubiquitous. The Second Factor Is Still a Credential.

by Nick Clark | Published March 28, 2026 | PDF

Duo Security made multi-factor authentication ubiquitous by providing push-based approval, biometric verification, and device health assessment through a simple integration model. The friction of MFA dropped significantly. But each authentication factor is a credential: the Duo Mobile app holds a registration secret, biometric templates are enrolled and stored, and hardware tokens carry cryptographic keys. More factors means more credentials. The structural gap is between multiplying credential types and eliminating the credential dependency entirely through identity derived from accumulated behavioral continuity.

Duo's contribution to making MFA accessible across enterprises and its device trust capabilities are genuine advances in security posture. The gap described here is about the credential model underlying all authentication factors.

More factors, more credentials

Duo adds a second factor to authentication: push notification, phone callback, SMS code, hardware token, or biometric. Each factor requires credential material. The Duo app must be enrolled with a registration secret. Biometric verification requires a stored template. Hardware tokens contain cryptographic seeds. The second factor is a second credential, not an escape from credentials.

When users lose their phone, change devices, or have their Duo registration compromised, they need to re-enroll. The identity was bound to the credential. When the credential is gone, identity verification fails until new credentials are provisioned.

Device trust evaluates the container, not identity

Duo's device trust feature evaluates whether the accessing device meets security requirements: OS version, disk encryption, screen lock. This is device health assessment. It verifies that the device is in a secure state. It does not verify that the device's identity derives from its own behavioral continuity.

A device that passes all health checks but has been factory-reset and re-enrolled is treated as the same identity. The identity is the enrollment, not the device's accumulated behavior.

What keyless identity addresses

Keyless identity would replace enrolled credentials with behavioral continuity. A device's identity would derive from its accumulated interactions validated through trust slope functions. No enrollment secret, no stored biometric template, no hardware token. The device proves it is the same device through continuity of behavior, not through possession of a credential.

Duo's adaptive access and device health capabilities could complement keyless identity by providing context signals. The identity primitive would shift from enrolled credentials to behavioral continuity.

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

Subject to one or more pending U.S. and international patent applications, see Patents for the current list and status. No license, express or implied, is granted. Any use requires a separate written agreement—see Licensing. Patent applications referenced on this site are pending. Claim scope, if any, is subject to examination and may issue in altered form or not at all. See Legal for terms and conditions.

Adaptive Query™ is a trademark of Nicholas Clark. U.S. federal registration is pending. federal registration. AQ™ , AQ Inside™ , Adaptive Index™ , Adaptive Network™ , Semantic Agent™ , @AQ™ , AQID™ , and Adaptive Coin™ are used as trademarks in connection with the Adaptive Query platform and brand. Other names may be trademarks of their respective owners.

Platform operated by Adaptive Query LLC, which provides patent and trademark licensing services. Copyright © 2025-2026 Nicholas Clark. All rights reserved.

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