Microsoft Entra Unified Cloud Identity. Identity Still Depends on Stored Credentials.

by Nick Clark | Published March 28, 2026 | PDF

Microsoft Entra ID unified enterprise identity across Azure, Microsoft 365, and third-party applications with conditional access policies, passwordless authentication methods, and verifiable credentials. The identity management is comprehensive. But every authentication flow ultimately terminates in a credential: a certificate, a FIDO2 key, a phone-based authenticator, or a biometric template matched against an enrolled record. The credentials are better protected than ever. They are still stored artifacts that can be compromised. The structural gap is whether identity can exist without persistent credentials, derived instead from accumulated behavioral continuity validated through trust slope functions.

Entra ID's conditional access engine, cross-cloud federation, and verified credentials initiative represent substantial investment in identity infrastructure. The gap described here is about the identity primitive, not about management quality.

Credentials are better protected, not eliminated

Entra ID offers passwordless authentication through Windows Hello, FIDO2 security keys, and the Microsoft Authenticator app. These reduce reliance on passwords. But they replace one credential type with another. A FIDO2 key stores a private key. Windows Hello stores a biometric template and a device-bound key. The Authenticator app stores registration secrets. The credentials changed form. They did not disappear.

Conditional access policies evaluate risk signals before granting access: device compliance, location, sign-in risk, and user risk. These policies add layers of validation around the credential. But the credential remains the foundation. Remove the credential and the identity system has nothing to authenticate against.

Verified credentials shift the format, not the model

Entra Verified Credentials implements decentralized identity standards, allowing users to present verifiable claims without exposing the underlying identity data. This is a genuine advance in privacy-preserving authentication. But verified credentials are still issued credentials: digital artifacts that were created at enrollment time and must be stored by the holder.

A verified credential that is lost, stolen, or revoked requires reissuance from the original issuer. The identity depends on the continued existence of the credential artifact. The format is better. The structural dependency on stored material persists.

What keyless identity addresses

Keyless identity derives identity from accumulated behavioral continuity rather than stored key material. A device proves its identity through a dynamic hash chain anchored in locally-sourced unpredictability, validated through trust slope continuity with its behavioral history. There is no credential to store, steal, or revoke. The identity primitive is the device's own continuity.

Entra's conditional access engine could evaluate trust slope continuity as an authentication signal alongside its existing risk signals. The identity primitive would shift from stored credentials to behavioral continuity, eliminating the class of attacks that depend on credential theft.

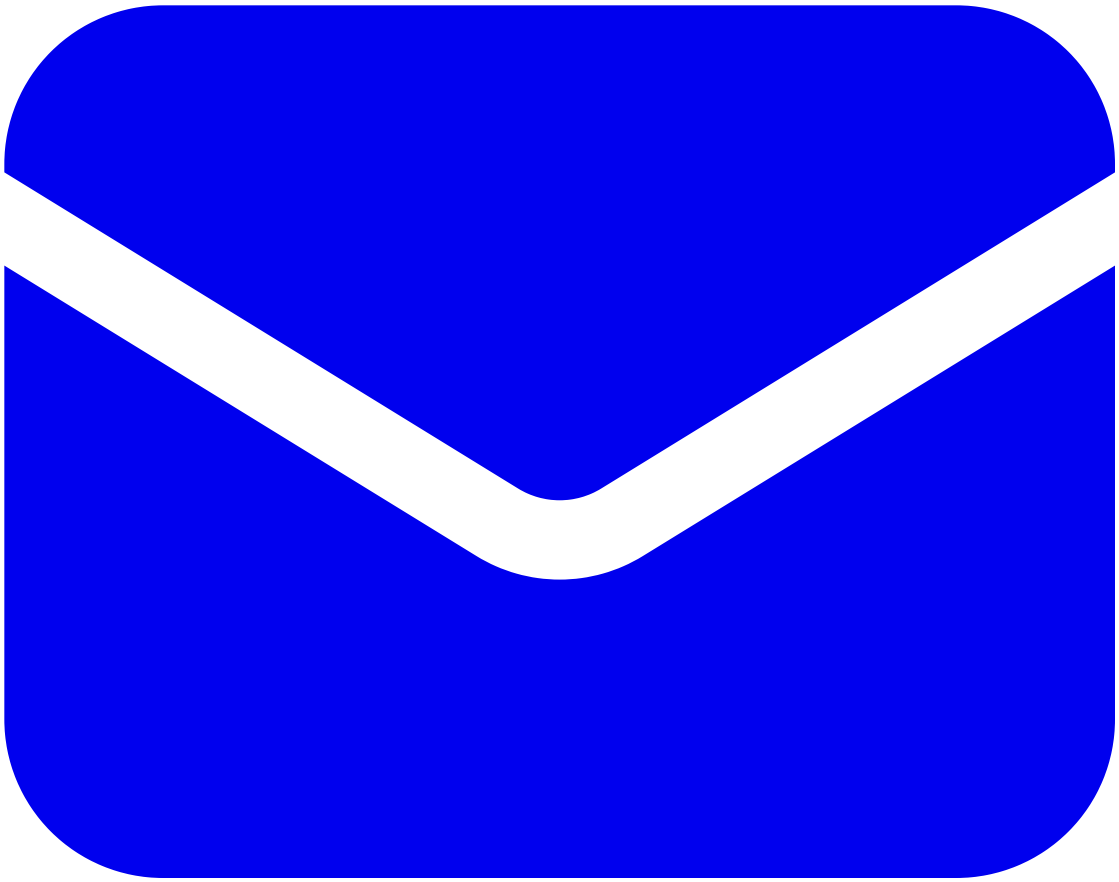
Keyless Identity All 21 steps →

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

and brand. Other names may be trademarks of their respective owners.

Last updated: 2026-03-03



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

Invented by Nick Clark | Founding Investors: Devin Wilkie