authID Launches Industry-First Quantum-Resistant Biometric Authentication Platform

April 24, 2026

PrivacyKey Platform Integrates NIST Post-Quantum Standards and MPC Cryptographic Key Protection to Eliminate Quantum Threats and Future-Proof Identity Security

Denver, April 24, 2026 (GLOBE NEWSWIRE) -- authID, a leader in biometric identity verification, today announced a landmark advancement in identity security: the quantum-hardening of its PrivacyKey™ biometric digital signature platform. This achievement represents the industry's first biometric authentication solution purpose-built to withstand the cryptographic threats posed by quantum computing.

Unlike conventional biometric systems that store facial templates on servers, leaving them vulnerable to future quantum-powered decryption attacks, authID's PrivacyKey™ architecture stores no biometric data at rest. Every authentication event regenerates an ephemeral cryptographic keypair from a live biometric presentation, signs the transaction, and immediately destroys the private key. The result is a biometric digital signature: a deterministic cryptographic proof that a specific individual was present at the exact moment a transaction was authorized.

"The quantum era is not a distant threat; it's an engineering reality today," said Rhon Daguro, CEO of authID. "NIST has finalized its standards, regulatory timelines are accelerating, and organizations that rely on legacy biometric architectures are already running out of time. We built PrivacyKey™ from the ground up on a zero-storage, ephemeral-key foundation precisely because we knew this day was coming. What we're announcing today isn't a patch or an upgrade. It's proof that the architecture we chose is the best one for the enterprise."

authID's engineering breakthrough represents two advances in quantum defense:

Quantum-Resistant Digital Signatures. PrivacyKey™ now supports three NIST-standardized post-quantum algorithms — ML-DSA-65, SLH-DSA-128s, and SLH-DSA-256s — spanning two independent mathematical foundations: lattice-based and hash-based cryptography. Organizations can select algorithms per operation, per policy, or per risk model, eliminating any single point of cryptographic failure.

Threshold MPC Key Protection (Sharding). Every PrivacyKeyMap™ (authID's encrypted biometric guidance artifact) is protected by a unique AES-256 key that is never stored whole. Instead, each key is sharded (divided) across multiple independent nodes in separate trust domains using a threshold multi-party computation ceremony. No single node ever holds the complete key. No single server breach, compromised administrator, or insider threat can reconstruct it. Authentication requires all distributed nodes to collaborate in real time, regenerating the key only for a specific operation as needed.

"Integrating NIST-standardized, post-quantum algorithms means our customers are protected even in scenarios where one cryptographic family is compromised," said Tom Szoke, founder and Chief Technology Officer of authID. "Combined with MPC and sharding, where no single node ever holds a complete key, we've created a system where the only path to authentication is a live person, in real time, collaborating with a distributed network. That's not just quantum-resistant. That's a fundamentally game-changing security model."

Quantum computing, while not completely realized, has been considered a severe cybersecurity threat to break commonly used methods for encrypting data, communications, and user identities. While some organizations are simply hoping to postpone the inevitability of quantum break-ins with longer encryption keys, it's theorized that the strongest quantum computer could infiltrate RSA-2048, the most powerful current encryption, in seconds. Since identities are the pathway for cyber-intruders, the need for quantum-resistant identity verification is more critical than ever.

"Our customers are making identity infrastructure decisions today that will define their security posture for the next decade," said Erick Soto, Chief Product Officer at authID. "PrivacyKey™ gives them the flexibility to choose their quantum algorithm per operation and per risk profile, without rearchitecting their workflows. The ability to enforce biometric-bound, quantum-hardened digital signatures at the transaction level is a capability no other platform offers. We're giving enterprises a way to get ahead of the quantum threat without waiting for it to arrive."

The quantum-resistant PrivacyKey™ platform is available now for enterprise customers seeking to future-proof their identity and authentication infrastructure. For the authID whitepaper on this solution, visit

https://authid.ai/downloads/authid-quantum-resistant-biometric-authentication.pdf

About authID Inc.

authID® (Nasdaq: AUID) ensures enterprises "Know Who's Behind the Device™" for every customer or employee login and transaction through its easy-to-integrate, patented, biometric identity platform. authID quickly and accurately verifies a user's identity, preventing cybercriminals from compromising account openings or taking over accounts. Leveraging a 1-in-1-billion False Positive Rate for the highest level of assurance, coupled with industry-leading speed and privacy-preserving technology, authID provides the most secure digital identity experience. authID's IDX platform secures the distributed workforce of employees, contractors, and vendors, as well as bringing authorization and accountability for AI agents. By creating a biometric root of trust for each user, authID stops fraud at onboarding, detects and stops deepfakes, eliminates password risks and costs, and provides the fastest, frictionless, and most accurate user identity experience in the industry. For more information, please visit www.authID.ai

authID Investor Relations
investor-relations@authID.ai