authID Mandate For Agentic AI

As enterprises embrace generative AI and autonomous agents, a new identity challenge emerges: machines now act on behalf of humans, yet operate without identity, oversight, or accountability. These agents are no longer tools—they're collaborators, decision-makers, and risk vectors.

authID Mandate is the first identity and security framework purpose-built for the agentic enterprise. It extends the chain of trust from human to machine, ensuring every AI agent is verifiably known, governed by policy, and accountable for its actions, per the scope of its human sponsor.

With Mandate, enterprises can confidently deploy autonomous agents while maintaining control, compliance, and trust, ushering in a new era of secure human–AI collaboration.

The New Identity Crisis: Challenges of Agentic AI

Enterprises have secured human identity, but autonomous AI introduces a new set of risks. AI agents often operate **anonymously**, making it difficult to verify authenticity, assign responsibility, or prevent unauthorized access. Traditional access controls and policies don't translate effectively, creating gaps in **authorization, accountability, and compliance**. Without immutable audit trails, organizations struggle to meet regulatory requirements and maintain operational confidence in AI-driven workflows.

Additionally, AI agents can be exploited for malicious purposes, including **prompt injection, API misuse, or unauthorized transactions**, which heightens security and operational risk. The lack of verifiable identity and traceable actions creates a **trust deficit** in human–AI collaboration, limiting the enterprise's ability to safely integrate autonomous agents into critical business processes. **Mandate addresses these challenges** by providing a complete lifecycle for identity, control, monitoring, and proof, extending enterprise trust from humans to AI agents.

Secure, Invoke and Audit AI Agents

Identify: Human users are biometrically verified and onboarded.

Register: Authorized agents are created in a secure registry.

Launch: Agents are invoked only in conjunction with a verified human sponsor's biometric credential. Mandate expresses Verifiable Credentials and JWT/VC-style claims over OAuth 2.1, OIDC, A2A, MCP, TAP, etc.

Audit: Mandate produces a cryptographically signed record that links the agent id with its human sponsor as well as its scope and with the exact action taken (eg. amount, resource, tool, timestamp, outcome).

Mandate: The Agentic AI Security Framework

Complete Lifecycle Security for Agentic AI

Why It's Different
Beyond Traditional IAM
Built for Agentic AI, not humans at keyboards., Mandate adds cryptographic human–agent binding and governance for autonomous decisions.

Autonomy with Accountability
Mandate in Action
Human verified once → issues biometric-backed credential. Agent acts autonomously, but every high-risk call proves identity, scope, and sponsorship.

Security Advantages
Unphishable Credentials
Replaces bearer tokens with short-lived, sender-constrained tokens tied to human sponsorship. Stops impersonation, replay, and over-scoping, and can revoke sponsor credentials.

Biometric Integration
Biometrics Without UI
Biometrics stay with the human. Downstream systems verify signatures and claims with no cameras required.

Contact Us www.authid.ai sales@authid.ai

authID Mandate For Agentic AI

Why Mandate?

Many organizations wanting to increase their productivity hesitate to deploy large-scale AI initiatives for lack of necessary governance. authID Mandate mitigates this gap through the biometric authorization of human sponsors and the accountability of AI agents.

Establish Verifiable Trust

Eliminate anonymity. Every agent is a **known, trusted entity,** and is only invoked by a biometrically-verified human.

Enforce Accountability

Every agent's action is **traceable to its owner** with **biometrically anchored audit trails**.

Mitigate AI-Driven Risk

Confidently manage **compliance, fraud, and operational risk.**

Enable Operational Confidence

Empower enterprises to safely deploy autonomous agents, knowing that **identity, authorization, and proof** are built-in.

Speed, Accuracy and Compliance

Proof verifies identities in just **700ms, 10 times faster** than traditional methods. With an industry-leading **false match rate of 1 in 1 billion**, our solution ensures unparalleled accuracy. Additionally, we support global compliance by ensuring that **no biometrics are stored,** prioritizing both security and privacy.

About authID

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, eliminating any assumption of 'who' is behind a1 device to prevent 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. Our IDX platform secures the distributed workforce of employees, contractors, and vendors, as well as bringing authorization and accountability for AI agents through our authID Mandate product line. 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.

Contact Us www.authid.ai sales@authid.ai